

NFC

Procedures



National Finance Center
Office of the Chief Financial Officer
U.S. Department of Agriculture

Updated August 2003

Security Access

TITLE VI
Systems Access Manual

CHAPTER 1
Agency Liaison And Security Access

SECTION 1
Security Access

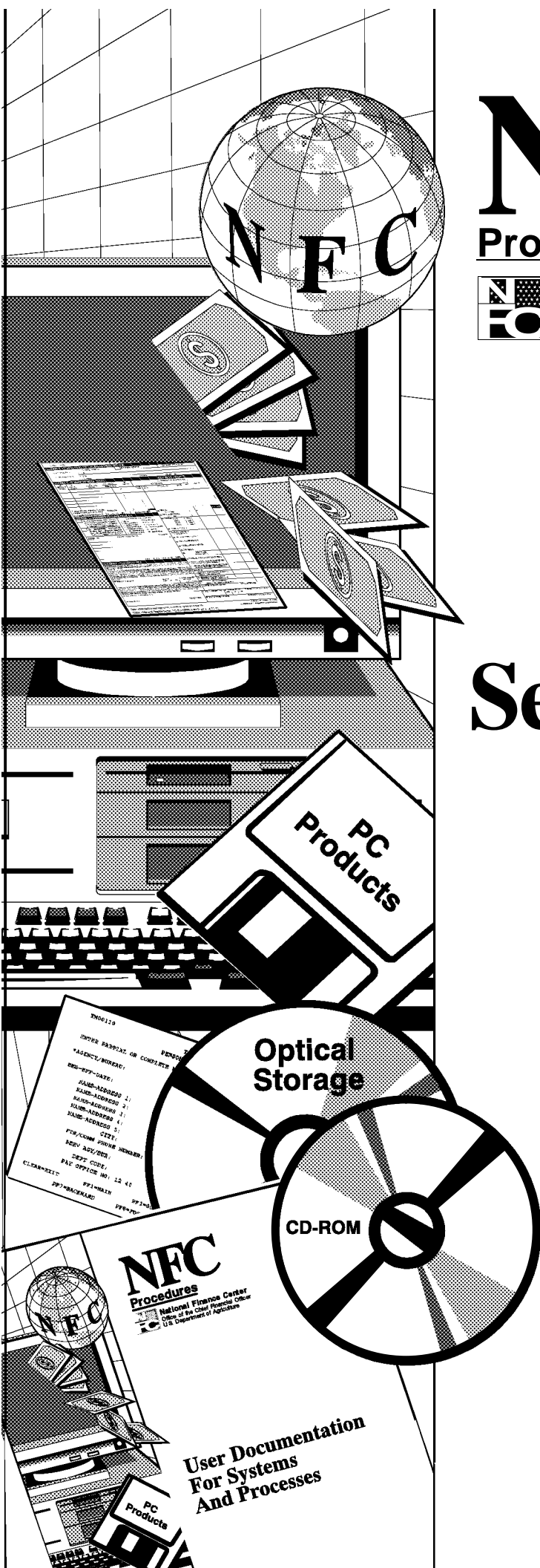


Table Of Contents

Introduction

<u>About This Procedure</u>	v
<u>How This Procedure Is Organized</u>	v
<u>What Conventions Are Used</u>	v
<u>Who To Contact For Help</u>	vi
<u>System Overview</u>	1
<u>Security Policy</u>	1
<u>Responsibilities</u>	1
<u>Access Administration</u>	2
<u>Access To Facilities</u>	2
<u>Access To Resources</u>	2
<u>Client Security Officer Activities</u>	3
<u>Establish User Access</u>	3
<u>Telephone Inquiries</u>	4
<u>Security Procedures</u>	4
<u>Password Procedures</u>	5
<u>New Password</u>	5
<u>Expired/Aging Password</u>	5
<u>Lost Password</u>	5
<u>Password Security</u>	5
<u>Reporting Problems</u>	5
<u>Requesting Resource Access</u>	5
<u>CA-Top Secret</u>	6
<u>Security Features</u>	6
<u>System Access</u>	7
<u>Remote Terminal Usage And Security</u>	7
<u>Sign-On</u>	7
<u>Sign-Off</u>	8
<u>Operating Features</u>	9
<u>Option Selection</u>	9
<u>Help Screens</u>	9
<u>ASO Panels Or ASO</u>	10

Processing Instructions

<u>ASO Primary Option Menu</u>	13
<u>Default</u>	15
<u>Batch</u>	16
<u>HELPAUDT</u>	17

<u>HELPTSS</u>	18
<u>HELPUTIL</u>	20
<u>TSSAUDIT</u>	22
<u>TSSBATCH</u>	23
<u>TSSLIST</u>	25
<u>TSSALPHA</u>	26
<u>TSSUTAUD</u>	27
<u>TSSUTDAY</u>	28
<u>TSSUTEXT</u>	30
<u>Output</u>	31
<u>Tutorial</u>	32
<u>Functions</u>	33
<u>Lock</u>	34
<u>Unlock</u>	34
<u>WHOAMI</u>	34
<u>Add Suspend</u>	35
<u>REM Suspend</u>	36
<u>REM Suspend & REP Password</u>	37
<u>REP Password</u>	38
<u>TSSLIST</u>	39
<u>Amatrix</u>	40
<u>Tutorial</u>	41
<u>Lists</u>	42
<u>TSSLIST</u>	42
<u>Access</u>	43
<u>Matrix</u>	43
<u>Officer</u>	44
<u>Print</u>	45
<u>Tutorial</u>	46
<u>Glossary</u>	48
<u>Messages</u>	50
<u>History</u>	52
<u>Standards</u>	53
<u>Tutorial</u>	54
<u>Access To FFIS</u>	56
<u>Background</u>	56
<u>Concept Of Security Operation</u>	57
<u>Procedure For Establishing And Defining Roles For FFIS Security</u>	57
<u>Procedures For Acquiring FFIS Access</u>	58
<u>Procedures For Changes To FFIS Access</u>	59

[Procedures For Requesting Deletion Of FFIS Access](#) 60

[Exhibits](#) 63

[1. FFIS Application Security Access Request Form](#) 65

[Instructions For Completing The FFIS Application Security Access Request Form](#) 66

[2. FFIS Application Security Access Specification Form](#) 67

[Instructions For Completing The FFIS Application Security Access Specification Form For The Form/Fort/Fors Tables](#) 68

[Glossary](#) 69

[Heading Index](#) *Index - 1*

About This Procedure

This procedure provides instructions for accessing and operating the National Finance Center's (NFC) computer facilities. The following information will help you use the procedure more effectively and locate further assistance if needed.

How This Procedure Is Organized

The primary sections of this procedure are described below:

[System Overview](#) describes what the system is used for and provides related background information.

[System Access](#) provides access security information and instructions for accessing the system.

[Operating Features](#) describes the system's design and how to use its operating features.

The [Main Menu](#) gives instructions for selecting the main options.

Instructions for each submenu and option are provided under a separate heading. All options on a submenu are described before going to the next option on the main menu. The screens for system menus and options are presented as figures within the text.

[Exhibits](#) include illustrations such as examples of FFIS Internal Security Access Request Form and FFIS Internal Security Access Specification Form with completion instructions for both forms.

[Glossary](#) (general) provides an explanation of the terminology of words that are used throughout this procedure.

Pages are numbered consecutively at the bottom.

You may occasionally receive bulletins to supplement information in this procedure. Each bulletin should be filed in front of the procedure and retained until the expiration date shown at the bottom of the bulletin.

What Conventions Are Used

This procedure uses the following conventions:

- Messages displayed by the system are printed in *italics*. Example: The message *3:49 pm* is displayed.
- Field specifications are also printed in *italics*. Example:

Enter User ID *required, alphanumeric; 8 positions max.*
Key in your assigned user ID (e.g., **NFXXX**).

- Data that you **must** key in exactly as shown is printed in bold italics. Example: Key in **1**.
- Figure references printed in **bold** link the figures with the text. Example: The NFC banner screen (**Figure 2**) is displayed.
- References to sections within the procedure are printed in **bold**. Example: See **Exhibit 1**.
- Keyboard references are printed in brackets ([**1**]). Example: Press **[Enter]**. Press **[PF6]**.
- Bullets (•) are used to emphasize a procedure. Example:
 - Memorize your user ID/password upon receipt.
- Important extra information is identified as a note. Example:

Note: The name TEST ACID and NFXXX are used for illustrative purposes only.

Who To Contact For Help

For questions about the system (including help with unusual conditions), contact Information Center personnel at **504-255-5230**.

For security related problems or obtaining access authority contact the Information Systems Security Office at **504-255-5407** .

For questions about this procedure, contact the Directives and Analysis Branch at **504-255-5322** .

System Overview

The Security Access procedure provides instructions for Client Security Officers to obtain authorization for their personnel to access the NFC's computer facilities.

The NFC's computer access control system is designed to provide protection for NFC's computer resources by (1) identifying users who have authorized access, (2) controlling the use of system facilities, (3) protecting and insuring the integrity of system resources, and (4) restricting the use of these resources. NFC will grant authority to access the computer facility to individual users at the request of their organization (transmitted through the client's Security Officer). Resource access permission is limited to the extent determined by the owner and the NFC. Types of access include reading the contents of a file, modifying the contents of a file, or executing a program.

Security Policy

USDA ADP Security Policy DR 3140 and the related ADP Security Manual DM 3140 require that managers of computer processing operations provide controlled access to the facilities and resources of the computer.

Users of a computing facility are to designate an ADP Security Officer (Client Security Officer) that is responsible for the management of access to the computer.

Responsibilities

Clients will appoint a Client Security Officer that coordinates all requests for NFC computer access authorization.

Client Security Officer will:

- Obtain organization and/or owner authorization approval(s) and establish user ID according to the client's ADP security policy.
- Submit the request for computer access to the NFC's ADP Security Officer.
- Suspend user ID upon the employee's termination or assignment change.
- Notify NFC of any changes in the authority or of the termination of an employee in their organization.
- Consult with NFC's Information Systems Security Officer (ISSO) on security matters related to the use of the NFC's facilities.
- Monitor client user activity for access violations.

NFC's Security Officer will:

- Grant authority to use/access the computer facilities based on the client's requirements.

- Establish, control, and maintain user identification.
- Log all unauthorized access attempts and furnish reports to the respective Client Security Officer for appropriate action.
- Monitor security concerns of the Client Security Officer related to the NFC's facilities and resources.

Access Administration

NFC will grant authority to use (access) its facilities to individual users at the request of their Client Security Officer. Every user will be assigned a unique identification which defines the specific information a user has access to based on job responsibilities, need to know, and the client's ADP security policy. Where appropriate, users are organized into functional groups based on their common access characteristics. The Client Security Officer is responsible for notifying NFC of any changes in their user groups. NFC logs any unauthorized access attempts and reports them to the Client Security Officer. If required, cancellations or suspensions of user identification should be handled immediately by telephoning the NFC ISSO. Communications relating to adds, deletes, or changes to user groups **must** go through the Client Security Officer to NFC. (See Communications for specific information on telephone or electronic communication with NFC.)

Access To Facilities

The NFC facilities are batch job processing (BATCH), time sharing options (TSO), integrated database management system (IDMS), and customer information control system (CICS) for automated transmission processing. Client personnel requiring access to NFC's computer facilities **must** identify their needs to the Client Security Officer.

All client personnel accessing NFC facilities are given an individual user identification Accessory ID (user ACID), which **must be** password protected. Each user is responsible for managing his/her own password when it expires (every 35 days) which he/she must change upon expiration or if the password is at risk.

Note: Accessor ID (user ACID) identifies both the user and the resources that the user is permitted to access. There are six major types of ACIDs; User, Profile, Department, Division, Zone, and Control.

Access To Resources

To access a given resource, a user **must** have permission to use the resource. Access to resources include files, databases, datasets, programs, terminals, nodes, etc. If access is being requested for resources that are owned by a client other than NFC, the requesting client **must** first obtain approval from the owner of the resource.

Client Security Officer Activities

The Client Security Officer submits requests for computer access, changes in authority, or termination of an employee, etc., to the NFC Information Systems Security Officer. The NFC Information Systems Security Officer implements the requests and notifies the Client Security Officer when completed.

Client Security Officers monitor and amend their security access profiles by coordinating with the NFC Information Systems Security Officer to establish a security access MATRIX for their particular agency.

The NFC Security Officer constructs the appropriate security access profiles based on each client's particular need for using the various applications of NFC's databases.

The sample of the Matrix (**Figure 1**) demonstrates how a client's requirements might evolve into various groupings of applications.

After clients define their groupings of applications, they establish the individual user's need-to-know capacity by identifying the range and extent of the organizational structure level that the user is authorized to query and/or input.

Security access authority (permission) is a function of the application groupings that are defined in the client combination matrix. Once the application combinations are determined, the range of data presented by the application is introduced. The grouping of these elements reside in a profile that is attached to the appropriate user ACID.

Establish User Access

The NFC ISSO establishes the access authority by interviewing the Client Security Officer. The communication with the Client Security Officer continues for administering additions and changes when necessary. The following describes the procedures the ISSO and the Client Security Officer follow when establishing the access authority and PROFILES for each client's organizational structure.

- Establish known sets of application combinations (groupings), as shown in the BROWSE - NFCPSECU.CLIENT.MATRIX (XXXX) sample screen (**Figure 1**).

```

BROWSE - NFCPSECU.CLIENT.MATRIX(XXXX) - 01.99 ----- LINE 00000000 COL 001 080
COMMAND ==> SCROLL BB=> CSR
***** TOP OF DATA *****
  XX/XX/xx AGENCY MATRIX PAGE 1 OF 10
APPLICATIONS A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
CULPRIT |X|X|X|X|X| |X|X|X|X|X|X|X|X| |X|X| |X|X|X|X|X|X|X|X|
PINQ |X| |X| | |X|X|X| | |X|X| | |X|X| | |X|X|X|X|
PINQ/S |X|X| | |X|X| |X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|
SINQ |X|X|X|X| |X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|
PRES |X|X|X|X| |X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|
RFQS | | | | | | | | | | | | | | | | | | | |
PMSO |X|X|X|X| |X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|
TRAI |X| | |X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|
TRAV | |X|X| |X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|X|

```

Figure 1. BROWSE - NFCPSECU.CLIENT.MATRIX (XXXX) Screen

- Consider the range of information determined by the Client's Organizational structure level.
- Decide each employee's need-to-know capacity and tailor these application combinations and their levels in the organizational structure.

PROFILES of the user access authority are available to the Client Security Officer and the NFC ISSO.

- PROFILES are structured as follows: P + AA + B + CCCC where:
P = PROFILE, AA = Agency Code (*), B = Application Combination Identifier (*),
CCCC = Intra Client Identity
- Note:** (*) This is normally the Personnel Office Identifier (POI) also referred to as Submitting Office Number (SON). A headquarters office may have total organizational access, an area office may only require access at the area level. Information contained in the PROFILE defines the exact range.

Telephone Inquiries

For questions about access authority, contact your Client Security Officer. When necessary, the Client Security Officer may contact the NFC Information Systems Security Officer at **504-255-5407**.

Security Procedures

Users are assigned a unique user ID and password. The user ID/password combination identifies the user to CA-Top Secret and allows him/her to access the resources required to perform your job. It is very important that the user ID/password be safeguarded. The following guidelines should be followed to secure your user ID.

Password Procedures

New Password

Must be at least six but not more than eight characters in length.

Expired/Aging Password

About 4 days prior to the automatic password expiration date, CA-Top Secret will display the message *TSS703W PASSWORD WILL EXPIRE SOON ON (mm/dd/yy)*, each time a user signs on to a facility.

Note: mm/dd/yy displays the month, day, and year that the password will expire.

Lost Password

If a user forgets his/her password, CA-Top Secret will not allow him/her to access a facility. Users should not attempt to guess passwords. Client Security Officers should be notified to receive a new password.

Password Security

To protect the password:

- Users should memorize their user ID/password upon receipt.
- Users should destroy all written records of their passwords. Do not post passwords or maintain them in an unprotected data set.
- Users do not share their user ID's or passwords with anyone. Personnel seeking the use of another's user ID/password combination should be directed to the appropriate security officer.
- Users should revise their passwords at regular intervals.
- Users are responsible for the use of the access authority contained on their user ID, therefore, they are responsible for the safeguarding of their user ID and password.

Reporting Problems

If violation messages are displayed:

- Do not clear the messages from the screen and do not press any keys on the keyboard.
- Copy all Top Secret Security (TSS) and message numbers and the accompanying text.
- Record all entries made prior to receiving the messages.
- Report the problem to the Client Security Officer.

Requesting Resource Access

Users should inform their supervisors if CA-Top Secret is prohibiting access to any resource that is necessary to perform their jobs.

Access to view, update, or delete data is determined by the agency security officer.

CA-Top Secret

CA-Top Secret is the access control software used by NFC to protect NFC's data processing resources. CA-Top Secret controls who can access certain resources and how and when those resources can be accessed. CA-Top Secret provides this protection by:

- Identifying users allowed to use the computing system
- Controlling access to system facilities
- Protecting and ensuring the integrity of resources
- Restricting the use of these resources

Components of CA-Top Secret include a security file (i.e., a security database), which describes user and resource access permission, a recovery file, and an audit tracking file.

Security Features

You can monitor security using the following Top Secret Security (TSS) features:

- **TSS LOCK/UNLOCK.** Use the TSS Lock command to lock an unattended terminal. To unlock a terminal, use the TSS Unlock command and enter your signon password when so requested by the system.
- **TSS Last-Used Message.** TSS displays the last-used message (TSS7011). This message informs you when, on which CPU, and through which facility your ACID was last used. It enables you to detect illegal use of your ACID.
- **TSS Status Message.** TSS status message informs how your session will be processed regarding security. It also contains a current count of the number of times your ACID was used.
- **TSS WHOAMI.** TSS message number TSS3031 contains the user's facility, terminal ID, system ID, and mode which can be helpful when reporting possible security problems.

System Access

To access the security CA-Top Secret functions of NFC systems, you must be established as an authorized Client Security Officer and use a terminal or personal computer that is connected to the mainframe computer. This section provides information on access security and gives specific sign-on/sign-off instructions.

Remote Terminal Usage And Security

To access the mainframe, use your telecommunications network (e.g., FTS2000, etc.). For information about connecting and disconnecting from your telecommunications network, see the instructions that are provided on your specific network.

Access security is designed to prevent unauthorized use of systems and databases. For information about access security, including user identification numbers (user ID's), passwords, and obtaining access to a specific system, see the Remote Terminal Usage procedure, Title VI, Chapter 2, Section 1.

Sign-On

To access NFC systems, display the NFC banner screen (**Figure 2**) on your terminal.

```

=====
SNAMOD2                      T3134605                      PF1=HELP
=====
NN      NN      FFFFFFFF      CCCCCCCC
NNN     NN      FFFFFFFF      CCCCCCCC
NNNN    NN      FF          CC
NNNN    NN      FFFFFFFF      CC
NN      NN      FFFFFFFF      CC
NN      NN      FF          CCCCCCCC
NN      NN      FF          CCCCCCCC
=====
National Finance Center
Office of the Chief Financial Officer
United States Department of Agriculture
=====
ENTER USER ID =          PASSWORD =          NEW PASSWORD =
ENTER APPLICATION NAME =          OR PRESS ENTER FOR NFC MENU
=====

```

Figure 2. NFC Banner Screen

Respond to the prompts as follows:

Enter User ID *required, alphanumeric; 8 positions max.*

Key in your assigned user ID (e.g., **NFXXX**).

Password *required, alpha; 6 to 8 positions*

Key in your password. Your password is not displayed on the screen.

New Password

optional, alpha; 6 to 8 positions

If your current password expires, key in a new password. Press **[Tab]**.

Enter Application Name

optional, alpha; 4 positions max.

Key in the application acronym i.e., **TSO**. Press **[Enter]**. If NFC needs to communicate special system function messages the Electronic Access Bulletin Board screen is displayed. Read the message(s) shown and press **[Enter]**.

The NFC Menu (**Figure 3**) is displayed.

```
=====
XX/XX/XX      SNAMOD2      NFC MENU      T3134806      15:12:50 CT
=====
SELECT ONE:
1. PAYROLL/PERSONNEL SYSTEMS
2. FINANCIAL INFORMATION SYSTEMS
3. PROPERTY MANAGEMENT INFORMATION SYSTEMS
4. ADMINISTRATIVE INFORMATION SYSTEMS
5. DEVELOPMENT SYSTEMS <NFC ONLY>
6. DATA BASE TEST SYSTEMS <NFC ONLY>
7. MISSION ASSIGNMENT TRACKING SYSTEM <GAO ONLY>
8. DIRECTIVES BULLETIN BOARD
ENTER APPLICATION NAME OR SELECTION NUMBER ==>      PF11 = EXIT
=====
MESSAGE BOARD
=====
```

Figure 3. NFC Menu

Press **[Enter]** again to display the first screen/menu in the application you have selected.

Sign-Off

To exit the Security Access system, press **[PF3]** at any screen. Continue pressing **[PF3]** until the TSO Ready *** prompt (**Figure 4**) is displayed. Key in **logoff** and press **[Enter]**.

```
Ready
***
logoff
```

Figure 4. Ready Prompt

The NFC Menu is displayed. You are now disconnected from the Security Access system. However, you are still connected to the mainframe and may select another application from the NFC Menu.

To disconnect from the mainframe, press **[PF11]** or a compatible function key. The NFC banner screen is displayed. If you do not intentionally disconnect from the mainframe, you are automatically disconnected after your terminal is inactive for a short time.

Note: To avoid unnecessary charges, disconnect from your telecommunications network immediately after the session is terminated. See Title VI, Chapter 2, Section 1, Remote Terminal Usage.

Operating Features

This section describes the basic operating features of the ADP Security Office (ASO) Panels.

Option Selection

To select an option from any menu, use one of two methods:

- Key in the option at the Option ==> prompt
- OR**
- With the cursor at the desired option, press **[Enter]**.

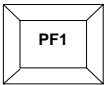
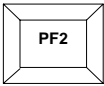
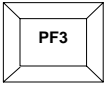
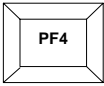

Help Screens

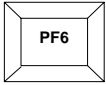
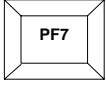
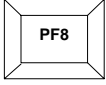
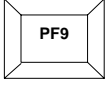
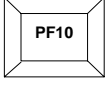
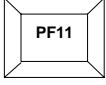
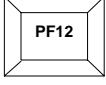
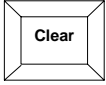
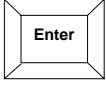

Help screens are available for all entry fields displayed on the screens. To obtain a Help screen, press **[PF5]** at any position on the screen. The Help screen is displayed and provides a description of the field either in narrative format or by listing the valid entry codes. Press **[Enter]** to return to the previous screen.

Function Keys

Program function keys are used to access system options. They are usually identified by **[PA]** (program attention), **[PF]** (program function), **[SF]** (special function), or **[SP]** (special program), depending on the equipment being used. Other function keys are **[Enter]**, **[Clear]**, and **[Tab]**. For detailed instructions on your equipment usage, see the appropriate manufacturer's operating guide. The functions of applicable PF keys are displayed at the bottom of each screen.

Function keys used in ASO panels are as follows:

Key	Description
	Used to receive help information on a specific screen, field, or function.
	Used to split or divide the screen.
	Used to end/exit the current screen.
	Used to return to the current screen.
	Used to repeat a find (Rfind) command that was entered while in the browse or the edit function.

Key	Description
	Used to repeat a change (Rchange) command that was entered while in the edit function.
	Used to scroll or browse up.
	Used to scroll or browse down.
	Used when you are in a split screen mode, the swap command jumps to the other logical screen.
	Used to move the screen to the left side for reports that are spread out beyond the screen's normal viewing parameters.
	Used to move the screen to the right side for reports that are spread out beyond the screen's viewing parameters.
	Used to recall previously entered command (Retrieve) to the command line. The commands are displayed one at a time in last-in first-out sequence. A command can be retrieved, edited, and resubmitted for processing.
	Used to exit the system from CICS.
	Used to enter (process) data.
	Used to move the cursor from field to field.

ASO Panels Or ASO

The ASO Panels or ASO are an ISPF Dialog consisting of CLIST's and panels developed to provide a simple, user-friendly environment for Client Security Officers to perform their jobs.

Several functions in the ASO panels now use the ISPF *BROWSE* feature to scroll through a listing and use the *FIND* command to locate a specific character string (i.e., user ID, profile, etc.).

Whenever the word *BROWSE* appears in the upper left corner of the screen, key in **FIND** *string-to-search-for* at the Command prompt (FIND may be shortened to F). Press **[Enter]**.

The ASO Panels can be accessed in any of the following ways:

- Key in **ASO** at the *TSO Ready* prompt.
- Key in **TSO ASO** at any Command (Command =>) or Option (Option =>) prompt in ISPF.

- Key in **ASO** at the TSO Command Processor prompt (option 6 on the ISPF/PDF Primary Option Menu). Press **[Enter]**.

The ASO banner screen is displayed, press **[Enter]** to display the ASO Primary Option Menu (**Figure 5**). However, if NFC needs to communicate special system function messages, the ASO Bulletin Board screen is displayed. Read the message(s) shown and press **[Enter]** again.

ASO Primary Option Menu

The ASO Primary Option Menu (**Figure 5**) provides ten options for selection.

```

----- ASO PRIMARY OPTION MENU -----
OPTION  ==>

      0  BATCH      - PERFORM BATCH PROCESS JOBS          USERID   - NFXXX
      1  FUNCTIONS  - PERFORM ONLINE COMMANDS            PROCEDURE- SECURE05
      2  LISTS      - PERFORM ONLINE LIST COMMANDS        PREFIX    - NFXXX
                                           TIME      - 10:30
                                           DATE      - 00/06/22
                                           JULIAN    - 00.174

      G  GLOSSARY   - GLOSSARY OF TSS TERMS
      M  MESSAGES   - COMMON TSS MESSAGES
      H  HISTORY    - HISTORY OF ASO BULLETIN BOARD MESSAGES
      S  STANDARDS  - STANDARDS FOR PASSWORD MANAGEMENT AND
                     USER ACCESS AUTHORIZATION

      D  DEFAULT    - SETUP DEFAULT PARAMETERS
      T  TUTORIAL   - DISPLAY ISPF HELP INFORMATION
      X  EXIT        - LEAVE ASO SECURITY FUNCTIONS

      HIT PF3 TO TERMINATE ASO DIALOG.

```

Figure 5. ASO Primary Option Menu

To select an option, key in your selection *number* or *letter* at the Option prompt. Press [Enter].

Below is a brief description of each option:

- 0** [BATCH](#) - Provides the ASO Batch Options Menu used to perform batch processing.
- 1** [FUNCTIONS](#) - Provides the ASO Functions Options Menu used to perform online commands.
- 2** [LISTS](#) - Provides the ASO List Options Menu used to perform online list commands.
- G** [GLOSSARY](#) - Provides the ASO Panels Glossary screen used to display the glossary of TSS terms.
- M** [MESSAGES](#) - Provides the ASO Panels TSS Messages screen used to describe the common TSS messages.
- H** [HISTORY](#) - Provides the ASOMSG - ASO Bulletin Board Message History Display Utility panel used to display prior messages from the history of ASO bulletin board messages.
- S** [STANDARDS](#) - Provides the BROWSE --NFCPSECU.Support.Standard screen used to display the standards for password management and user access authorization.
- D** [DEFAULT](#) - Provides the ASO Default screen used to setup default parameters.
- T** [TUTORIAL](#) - Provides the ISPF Tutorial screen used for displaying ISPF Help information.

X **EXIT** - Used to exit ASO security functions. Instructions to exit at any screen are provided in **Sign-Off** under **System Access**.

Instructions follow for using the system options. Although Option D, Default, is listed near the bottom of the ASO Primary Option Menu, the defaults must be set up before continuing on to the next option. Therefore, instructions for using Option D are provided before all other options.

Default

Default is Option D on the ASO Primary Option Menu (**Figure 5**). This option is used to setup default parameters.

Note: Although the default option is listed near the bottom of the ASO Primary Option Menu, the defaults must be set up before continuing on to the next option.

To select this option, key in **D** at the Option prompt. Press **[Enter]**.

The ASO Default screen (**Figure 6**) is displayed.

ASO DEFAULT

REL 1.0

DESTINATION INFORMATION (NO QUOTES) ==>
(i.e., JOHN DOE @ 255-5407)

ROUTE (REMOTE - YOUR LOCAL - ID) ==>
(i.e., U123)

MESSAGE CLASS
(X=OUTPUT TO TERMINAL, A=PRINT) ==>

JOB CARD INFORMATION:

LINE1: ==>
LINE2: ==>
LINE3: ==>
LINE4: ==>

HIT ENTER TO CONTINUE OR PF3 TO CANCEL

Figure 6. ASO Default Screen

Complete the fields as described:

- Destination Information

optional, alphanumeric; 20 positions max.
Key in your specific destination information.
- Route

optional, alphanumeric; 5 positions max.
Key in your local printer ID.
- Message Class

optional, alpha; 1 position
Key in **A** to have your batch job automatically sent to the printer without online retention **or** an **X** to allow the output of your batch job to be displayed at your terminal. If left blank, the system defaults to X. Press **[Enter]**.
- Jobcard Information:

After pressing **[Enter]**, the jobcard information is automatically filled out for you. As you change options in blocks 1, 2, or 3, this information will be updated, when pressing **[Enter]**.

Batch

Batch is Option 0 on the ASO Primary Option Menu (**Figure 5**). This menu is used to perform batch processing.

To select this option, key in **0** at the Option prompt. Press **[Enter]**.

The ASO Batch Options Menu (**Figure 7**) is displayed.

OPTION		ASO BATCH OPTIONS MENU	REL 1.0
===>			
0	HELPAUDT	HELP WITH TSS AUDIT COMMANDS	
1	HELPTSS	HELP WITH TSS COMMANDS	
2	HELPUTIL	HELP WITH TSS UTILITY FUNCTIONS	
3	TSSAUDIT	TSS AUDIT REPORT - CHANGES MADE TO SECURITY FILE	
4	TSSBATCH	RUN TSS COMMANDS FROM BATCH	
5	TSSLIST	SUMMARIZED LISTINGS OF USER AND PROFILE ACIDS	
6	TSSALPHA	ALPHA LISTING BY NAME OF YOUR ORGANIZATION'S USERS	
7	TSSUTAUD	VIOLATIONS FOR TODAY (WITHIN YOUR SCOPE)	
8	TSSUTDAY	ACCESS TO NFPC.FOCS FILES PREVIOUS 3 DAYS (W/I SCOPE ONLY)	
9	TSSUTEXT	VIOLATIONS/AUDIT EVENTS (W/I SCOPE ONLY)	
10	OUTPUT	VIEW/PRINT JOB OUTPUT	
T	TUTORIAL	DISPLAY ISPF HELP INFORMATION	
X	EXIT	LEAVE ASO SECURITY FUNCTIONS	
HIT PF3 TO RETURN TO ASO PRIMARY OPTION MENU			

Figure 7. ASO BATCH Options Menu

To select an option, key in the selection *number* or *letter* at the Option prompt. Press **[Enter]**.

Below is a brief description of each option:

- 0** [HELPAUDT](#) - Provides help with the TSS Audit commands.
- 1** [HELPTSS](#) - Provides help with the TSS commands.
- 2** [HELPUTIL](#) - Provides help with the TSS utility functions.
- 3** [TSSAUDIT](#) - Used to run audit reports for changes made to the security file by Security Officers.
- 4** [TSSBATCH](#) - Used to run batch jobs that execute TSS commands.
- 5** [TSSLIST](#) - Used to run a batch job that produces a summarized listing of the user and profile ACID's.
- 6** [TSSALPHA](#) - Used to run a batch job that produces an alphabetic listing of your organization's users by name.
- 7** [TSSUTAUD](#) - Used to run a batch job that produces a report showing user violations for Today.

- 8** [TSSUTDAY](#) - Used to run a batch job that produces a report showing which users accessed NFCP.FOCS file or a selected dataset file for the previous 3 days.
- 9** [TSSUTEXT](#) - Used to run a batch job that produces a report of violations and audited events for users for the previous 3 days.
- 10** [OUTPUT](#) - Used to allow viewing of output from BATCH jobs you have submitted with the capability to delete the output or route to a printer.
- T** [TUTORIAL](#) - Provides the ISPF Tutorial screen used for displaying ISPF Help information.
- X** [EXIT](#) - Used to exit ASO security functions. Instructions to exit at any screen are provided in **Sign-Off** under **System Access**.

HELPAUDT

HELPAUDT is Option 0 on the ASO Batch Options Menu (**Figure 7**). This option provides help with TSS audit commands.

To select this option, key in **0** at the Option prompt. Press **[Enter]**.

The BROWSE -- NFCPSECU.SECOFF.NFC (HELPAUDT) screen (**Figure 8**) is displayed.

```

BROWSE      NFCPSECU.SECOFF.NFC(HELPAUDT) - 01.04      Line 00000000 Col 001 080
COMMAND ==>                                SCROLL ==> PAGE
***** Top of Data *****
Control statements to be executed by the TSSAUDIT program.

CHANGES CONTROL STATEMENT
-----
Lists changes made to the TOP SECRET security file.

-----
CHANGES  CA(acid)  DATE(-nn)  STRING(string)
-----
CA          Only those changes made by the indicated control
            ACID are to be listed.  If omitted, all changes are
            listed.

DATE       Relative displacement (in days) from the current
            date.  This displacement is subtracted from the
            current date to get a starting date for the search
            of the recovery file.  TSSAUDIT then lists only
            those changes made on or after the starting date.

```

Figure 8. BROWSE -- NFCPSECU.SECOFF.NFC (HELPAUDT) Screen

At the Command prompt, key in the control statement changes to be executed by the TSSAUDIT program.

Note: Press **[PF8]** to display the next screen (**Figure 9**) which gives you examples and an explanation of what to enter at the Command prompt.


```

BROWSE      NFCPSECU.SECOFF.NFC(HELPAUDT) - 01.04      Line 00000019 Col 001 080
COMMAND ==>                                     SCROLL ==> PAGE
          If omitted, no date restrictions are applied.

      STRING      Only those changes containing the specific string
                  are listed.

PRIVILEGES CONTROL STATEMENT
-----
Lists security file information about one or more ACIDS.
-----

      PRIVILEGES SHORT

-----

      SHORT      Information is listed only for those ACIDS that have
                  administrative authority or attributes AUDIT or SUSPEND.

EXAMPLES:

CHANGES CA(vca01) DATE(-05) STRING(TSS REM)

```

Figure 9. BROWSE--NFCPSECU.SECOFF .NFC (HELPAUDT) Screen (cont'd)

Note: Press **[PF8]** to display the next screen (**Figure 10**). After you key in the control statement changes, press **[Enter]**.

```

BROWSE      NFCPSECU.SECOFF.NFC(HELPAUDT) - 01.04      Line 00000038 Col 001 080
COMMAND ==>                                     SCROLL ==> PAGE
List all occurrences of the string 'TSS REM' that were made by vca01
beginning from the previous 5 days.
-----
PRIVILEGES SHORT
List all ACIDS that have administrative authority or have the attribute
AUDIT or SUSPEND.
-----
***** Bottom of Data *****

```

Figure 10. BROWSE -- NFCSECU.SECU.SECOFF.NFC (HELPAUDT) Screen (cont'd)

HELPTSS

HELPTSS is Option 1 on the ASO Batch Options Menu (**Figure 7**). This option provides help with TSS commands.

To select this option, key in **1** at the Option prompt. Press **[Enter]**.

The BROWSE -- NFCPSECU.SECOFF.NFC (HELPTSS) screen (**Figure 11**) is displayed.

```

BROWSE      NFCPSECU.SECOFF.NFC(HELPTSS) - 01.00          Line 00000000 Col 001 080
COMMAND ==>                                         SCROLL ==> PAGE
***** TOP OF DATA *****
THE FOLLOWING IS A MENU OF TSS COMMAND FUNCTIONS.
ADDTO      Add attributes to user acids.
           FORMAT: TSS ADD(acid) SUSPEND
REMOVE     Removes attributes from user acids.
           FORMAT: TSS REM(acid) SUSPEND
REPLACE    Replaces attributes of existing ACID.
           FORMAT: TSS REP(acid) PASSWORD(new password,35,exp)
LOCK       Lock a terminal.
           FORMAT: TSS LOCK
UNLOCK     Unlock a terminal
           FORMAT: TSS UNLOCK
WHOAMI     Display current user status
           FORMAT: TSS WHOAMI

```

Figure 11. BROWSE --NFCPSECU.SECOFF.NFC (HELPTSS) Screen

Key in the applicable TSS command function at the Command prompt, using the format listed below. Press **[Enter]**.

Note: The command must be prefixed with TSO if entered from this screen, i.e., TSO TSS ADD (acid) SUSPEND.

- ADDTO** - Add attributes to user ACIDs.
FORMAT:TSS ADD (acid) SUSPEND
- REMOVE** - Removes attributes from user ACIDs.
FORMAT: TSS REM (acid) SUSPEND
- REPLACE** - Replace attributes of existing ACID.
FORMAT: TSS REP (acid) PASSWORD (new password, 35, exp).
- LOCK** - Lock a terminal.
FORMAT: TSS LOCK
- UNLOCK** - Unlock a terminal
FORMAT: TSS UNLOCK
- WHOAMI** - Display current user status.
FORMAT: TSS WHOAMI

Note: Press **[PF8]** to display the next screen (**Figure 12**), which gives you an explanation of what to enter at the Command prompt.

```

BROWSE      NFCPSECU.SECOFF.NFC(HELPTSS) - 01.00          Line 00000019 Col 001 080
COMMAND ==>                                         SCROLL ==> PAGE

LIST      List security record(s) of an acid
          FORMAT:  TSS LIST(acid) DIV(division name) DEPT(dept name)
                  TYPE(acid-type) DATA(see list)
          ALL - List all information
          NA - List only name
          BA - List only basic information
          AC - List only user acids
          IN - List only installation data
          US - List only user ACIDS
          PR - List only profile ACIDS
          ***** Bottom of Data *****

```

Figure 12. BROWSE -- NFCPSECU.SECOFF.NFC (HELPTSS) Screen (cont'd)

LIST List security record(s) of an ACID. (*See list*):

ALL	-	List all information
NA	-	List only name
BA	-	List only basic information
AC	-	List only user ACIDS
IN	-	List only installation data
US	-	List only user ACIDS
PR	-	List only profile ACIDS

After you key in the applicable TSS command function, press **[Enter]**.

HELPUTIL

HELPUTIL is Option 2 on the ASO Batch Options Menu (**Figure 7**). This option provides help with TSS utility functions.

To select this option, key in **2** at the Option prompt. Press **[Enter]**.

The BROWSE -- NFCPSECU.SECOFF.NFC (HELPUTIL) screen (**Figure 13**) is displayed.

```

BROWSE      NFCPSECU.SECOFF.NFC(HELPUTIL) - 01.12      Line 00000000 Col 001 080
COMMAND ===>                                         SCROLL ===> PAGE
***** Top of Data *****
The following keywords can be used in executing UTIL reports.

REPORT      Requests activity/violation report.
END         Delimits multiple reports.
EVENT      Selects type of event:
           ALL      = All events
           ACCESS   = Resource accesses
           VIOL     = Violations
           INIT     = Job/session initiations
           TERM     = Job/session terminations
ACID(acid)  Selects activity for a given acid.
DEPT(acid)  Selects activity within department.
JOB(job-list) Job/session(s).
FACILITY    Facilities.
DATE(yyddd) Julian date range.
DATE(TODAY) Today's SMF records.
DATE(-nn)   Previous "nn" days' SMF records.
TIME(hhmmss) Time period.
DATASET     Data set prefixes.

```

Figure 13. Browse -- NFCPSECU.SECOFF.NFC (HELPUTIL) Screen

Note: Press **[PF8]** to display the next screen (**Figure 14**) which gives you examples and an explanation of what to enter at the Command prompt.

```

BROWSE      NFCPSECU.SECOFF.NFC(HELPUTIL) - 01.12      Line 00000020 Col 001 080
COMMAND ===>                                         SCROLL ===> PAGE
VOLUME      Volume prefixes.
CLASS(Y)    IDMS schema/subschema
CLASS(a)    TSS subschema (must be lower case 'a', not 'A')
CLASS(K)    Terminal unlocks
RES(?) CLASS(T) Terminal
TITLE       Title line

EXAMPLES:

REPORT EVENT(VIOL) END
REPORT EVENT(AUDIT) END
Produces two reports, the first a total violation report and a second
report that produces audit entries.
-----
EVENT(ACCESS) ACID(ACID01) DATE(90215,90215) TIME(063000,090000)
Selects all accesses by user ACID01 on 08/03/90 from 06:30 - 09:00 a.m.
-----
EVENT(VIOL) DEPT(ABCDEPT) DATE(90215,90215)
Selects all violations by users in the ABCDEPT department on 08/03/90
-----

```

Figure 14. .BROWSE -- NFCPSECU.SECOFF.NFC (HELPUTIL) Screen (cont'd)

Note: Press **[PF8]** to display the next screen (**Figure 15**). After you key in the command for executing UTIL reports, press **[Enter]**.

```

BROWSE      NFCPSECU.SECOFF.NFC(HELPUTIL) - 01.12      Line 00000040 Col 001 080
COMMAND ==>                                     SCROLL ==> PAGE
EVENT(VIOL) CLASS(K)
Selects all unsuccessful terminal unlocks
-----
EVENT(ACCESS) D(NFCP.FOCS.FS2.EXEC) DATE(-02)
Selects all access to dataset NFCP.FOCS.FS2.EXEC by users from the
previous 2 days.
-----
EVENT(INIT) RES(R15.RD1) CLASS(T)
Selects all jobs submitted from terminal R15.RD1
-----
***** Bottom of Data *****

```

Figure 15. BROWSE -- NFCPSECU.SECOFF.NFC (HELPUTIL) Screen (cont'd)

TSSAUDIT

TSSAUDIT is Option 3 on the ASO Batch Options Menu (Figure 7). This option is used for TSS changes made to the security files.

To select this option, key in **3** at the Option prompt. Press **[Enter]**.

The ASO Batch - TSSAUDIT screen (Figure 16) is displayed.

```

-----
ASO BATCH - TSSAUDIT      (CHANGES MADE TO SECURITY FILE)      REL 1.0

DESTINATION INFORMATION      ==>
ROUTE (REMOTE - YOUR LOCAL - ID) ==>
MESSAGE CLASS
(X=OUTPUT TO TERMINAL, A=PRINT) ==>
OUTPUT REPORT TO DATASET (Y/N) ==>  N
NFXXX.TSSAUDIT

ACID FOR WHICH CHANGES ARE TO
BE REPORTED                  ==>  NFXXX

STRING FOR WHICH CHANGES ARE
TO BE REPORTED
(I.E., PROFILE NAME, DATASET) ==>

NUMBER OF DAYS TO REPORT ON  ==>  -1

```

Figure 16. ASO BATCH - TSSAUDIT Screen

The values shown are default values from the ASO Default screen. The values may be modified for the execution of the function. Complete the fields as described:

Destination Information *conditional field*

Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.

Route	<i>conditional field</i> Data is generated from the default parameters previously set-up or may be modified for the execution of this Job only.
Message Class	<i>conditional field</i> Data is generated from the default parameters previously set-up or may be modified for the execution of this Job only.
Output Report To Dataset (Y/N)	<i>optional, alpha; 1 position</i> Key in Y (yes) if you want the output report to go to dataset or N (no) if you do not want the output report to go to dataset. The system defaults to N .
ACID For Which Changes Are To be Reported	<i>optional, alphanumeric; 8 positions max.</i> Key in the user ID for a Departmental Security Administrator (DCA), this can be your user ID or another DCA in your department. For a Divisional Security Administrator (VCA), this can be your user ID, another VCA in your division, or the ACID of a DCA within your division.
String For Which Changes Are To Be Reported	<i>optional, alphanumeric; 8 positions max.</i> Key in a character string to specify a search for (e.g., profile P00SCRTY).
Number Of Days To Report On	<i>required, numeric; 3 positions max.</i> Key in specific starting date (i.e., -00 to -99) to report on. Example: -00 is today, -01 is yesterday, etc.

When all applicable fields are completed, press **[Enter]**.

TSSBATCH

TSSBATCH is Option 4 on the ASO Batch Options Menu (**Figure 7**). This option is used to run TSS commands from batch.

To select this option, key in **4** at the Option prompt. Press **[Enter]**.

The ASO Batch - TSSBATCH screen (**Figure 17**) is displayed. The values shown are default values from the ASO Default screen. The values may be modified for the execution of the function.

```

-----
ASO BATCH - TSSBATCH          (RUN TSS COMMANDS FROM BATCH)          REL 1.0

DESTINATION INFORMATION          ===>

ROUTE (REMOTE - YOUR LOCAL - ID)  ===>

MESSAGE CLASS
(X=OUTPUT TO TERMINAL, A=PRINT)  ===>

OUTPUT REPORT TO DATASET (Y/N)    ===>  N
NFXXX.TSSBATCH

NEED MORE THAN FIVE LINES ? (Y/N) ===>  N

YOU MAY CONTINUE A COMMAND BY PLACING A '-' AT THE END OF THE LINE

L1:
L2:
L3:
L4:
L5:

```

Figure 17. ASO BATCH - TSSBATCH Screen

Complete the fields as described:

- Destination Information** *conditional field*
Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.
- Route** *conditional field*
Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.
- Message Class** *conditional field*
Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.
- Output Report To Dataset (Y/N)** *optional, alpha; 1 position*
Key in **Y** (yes) if you want the output report to go to dataset or **N** (no) if you do not want the output report to go to dataset. The system defaults to **N**.
- Need More Than Five Lines? (Y/N)** *optional, alpha; 1 position*
Key in **Y** (yes) if you need more than five lines. If you key in **Y**, you may continue a command by keying in a **-** at the end of the line. The system defaults to **N**.

When all applicable fields are completed, press **[Enter]**.

TSSLIST

TSSLIST is Option 5 on the ASO Batch Options Menu (**Figure 7**). This option is used to summarize a listing of user and profile ACID's.

To select this option, key in **5** at the Options prompt. Press **[Enter]**.

The ASO Batch - TSSLIST screen (**Figure 18**) is displayed.

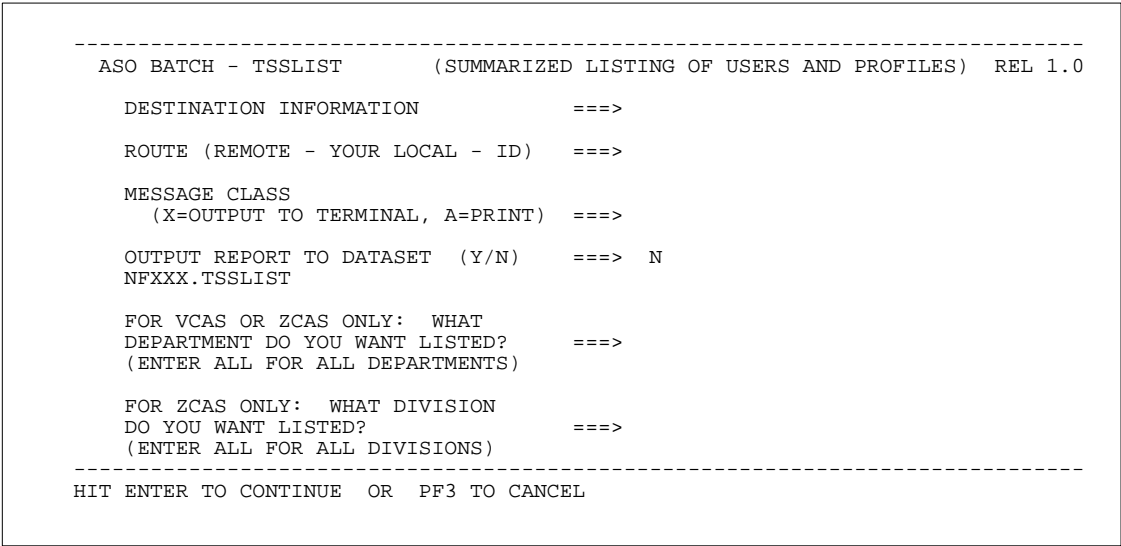


Figure 18. ASO BATCH - TSSLIST Screen

The values shown on the screen are default values from the ASO Default screen. The values may be modified for the execution of this function.

Complete the fields as described:

- Destination Information

conditional field
Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.
- Route

conditional field
Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.
- Message Class

conditional field
Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.
- Output Report To Dataset
(Y/N)

optional, alpha; 1 position
Key in **Y** (yes) or if you want the output report to go to dataset or **N** (no) if you do not want the output report to go to dataset. The system defaults to *N*.

**For VCAS Or ZCAS Only:
What Department Do You
Want Listed? (Enter All
For All Departments)**

optional, alpha; 3 positions max.

Key in the department you want listed **or** key in **a11** for all departments.

**For ZCAS Only: What
Division Do You Want
Listed? (Enter All For All
Divisions)**

optional, alpha; 3 positions max.

Key in the division you want listed **or** key in **a11** for all divisions.

When all applicable fields are completed, press **[Enter]**.

TSSALPHA

TSSALPHA is Option 6 on the ASO Batch Options Menu (**Figure 7**). This option is used to produce an alphabetical listing of your organization's users by name.

To select this option, key in **6** at the Option prompt. Press **[Enter]**.

The ASO BATCH - TSSALPHA screen (**Figure 19**) is displayed.

```

-----
ASO BATCH - TSSALPHA          (LISTING OF ORGANIZATION USERS BY NAME)      REL 1.0
DESTINATION INFORMATION          ===>
ROUTE (REMOTE - YOUR LOCAL - ID)  ===>
MESSAGE CLASS
  (X=OUTPUT TO TERMINAL, A=PRINT)  ===>
OUTPUT REPORT TO DATASET  (Y/N)    ===>  N
NFXXX.TSSALPHA

-----
HIT ENTER TO CONTINUE OR PF3 TO CANCEL
  
```

Figure 19. ASO BATCH - TSSALPHA Screen

The values shown on the screen are default values from the ASO DEFAULT screen. The values may be modified for the execution of this function.

Complete the fields as described:

Destination Information *conditional field*

Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.

Route	<i>conditional field</i> Data is generated from the default parameters previously set-up or may be modified for the execution of this Job only.
Message Class	<i>conditional field</i> Data is generated from the default parameters previously set-up or may be modified for the execution of this Job only.
Output Report To Dataset (Y/N)	<i>optional, alpha; 1 position</i> Key in Y (yes) if you want the output report to go to dataset or N (no) if you do not want the output report to go to dataset. The system defaults to <i>N</i> . Press [Enter] .

TSSUTAUD

TSSUTAUD is Option 7 on the ASO Batch Options Menu (**Figure 7**). This option is used to identify current user violations.

To select this option, key in **7** at the Option prompt. Press **[Enter]**.

The ASO Batch - TSSUTAUD screen (**Figure 20**) is displayed.

```
-----
ASO BATCH - TSSUTAUD          (VIOLATION TODAY)                      REL 1.0
DESTINATION INFORMATION          ===>
ROUTE (REMOTE - YOUR LOCAL - ID) ===>
MESSAGE CLASS
(X=OUTPUT TO TERMINAL, A=PRINT) ===>
OUTPUT REPORT TO DATASET (Y/N)  ===>  N
NFXXX.TSSUTAUD
TITLE FOR REPORT (40 CHAR. MAX)
===>
(DEFAULT IS "SPECIAL REPORT")
ACID TO REPORT ON                ===>
(DEFAULT IS ALL ACIDS)
-----
HIT ENTER TO CONTINUE OR PF3 TO CANCEL
```

Figure 20. ASO BATCH - TSSUTAUD Screen

The values shown on the screen are default values from the ASO Default screen. The values may be modified for the execution of this function.

Complete the fields as described:

Destination Information	<i>conditional field</i> Data is generated from the default parameters previously set-up or may be modified for the execution of this Job only.
Route	<i>conditional field</i> Data is generated from the default parameters previously set-up or may be modified for the execution of this Job only.
Message Class	<i>conditional field</i> Data is generated from the default parameters previously set-up or may be modified for the execution of this Job only.
Output Report To Dataset (Y/N)	<i>optional, alpha; 1 position</i> Key in Y (yes) if you want the output report to go to dataset or N (no) if you do not want the output report to go to dataset. The system defaults to <i>N</i> .
Title For Report (40 Char. Max)	<i>optional, alphanumeric; 40 positions max.</i> Key in the desired report title. The system default is <i>Special Report</i> .
ACID To Report On	<i>optional, alphanumeric, 8 positions max.</i> Key in the specific user ID you want to report on. If left blank, the system defaults to all <i>ACIDS</i> within your administrative scope of authority.

When all applicable fields are completed, press **[Enter]**.

TSSUTDAY

TSSUTDAY is Option 8 on the ASO Batch Options Menu (**Figure 7**). This option is used to report on access to your NFCP.FOCS datasets or a dataset that you specify for the previous three days.

To select this option, key in **8** at the Option prompt. Press **[Enter]**.

The ASO Batch - TSSUTDAY screen (**Figure 21**) is displayed.

```
-----
ASO BATCH - TSSUTDAY          (LIST OF USERS ACCESSING FOCUS FILES)      REL 1.0

DESTINATION INFORMATION          ===>

ROUTE (REMOTE - YOUR LOCAL - ID)  ===>

MESSAGE CLASS
(X=OUTPUT TO TERMINAL, A=PRINT)  ===>

OUTPUT REPORT TO DATASET  (Y/N)  ===>  N
NFXXX.TSSUTDAY

TITLE FOR REPORT (40 CHAR. MAX)
===>
(DEFAULT IS "SPECIAL REPORT" )

ACID TO REPORT ON                ===>
(DEFAULT IS ALL ACIDS)

DATASET TO REPORT ON             ===>
(DEFAULT IS "NFCP.FOCS" )
```

Figure 21. ASO BATCH - TSSUTDAY Screen

The values shown on the screen are default values from the ASO Default screen. The values may be modified for the execution of this function.

Complete the fields as described:

- Destination Information

conditional field
Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.
- Route

conditional field
Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.
- Message Class

conditional field
Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.
- Output Report To Dataset
(Y/N)

optional, alpha; 1 position
Key in **Y** (yes) if you want the output report to go to dataset or **N** (no) if you do not want the output report to go to dataset. The system defaults to *N*.
- Title For Report (40 Char.
Max)

optional, alphanumeric; 40 positions max.
Key in the desired report title. If left blank, the system defaults to *Special Report*.
- ACID To Report On

optional, alphanumeric, 8 positions max.
Key in the specific *user ID* you want to report on. If left blank, the system defaults to all *ACIDs* within your administrative scope of authority.

Dataset To Report On *optional, alphanumeric; 10 positions max.*

Key in the specific dataset you want to report on. If left blank, the system defaults to *NFCP.FOCS*.

When all applicable fields are completed, press **[Enter]**.

TSSUTEXT

TSSUTEXT is Option 9 on the ASO Batch Options Menu (**Figure 7**). This option is used to report on violations/audit events.

To select this option, key in **9** at the Option prompt. Press **[Enter]**.

The ASO Batch - TSSUTEXT screen (**Figure 22**) is displayed.

```

-----
ASO BATCH - TSSUTEXT          (VIOLATION/AUDIT REPORT)          REL 1.0
-----
DESTINATION INFORMATION      ===>
ROUTE (REMOTE - YOUR LOCAL - ID)  ===>
MESSAGE CLASS
(X=OUTPUT TO TERMINAL, A=PRINT)  ===>
OUTPUT REPORT TO DATASET  (Y/N)  ===>  N
NFXXX.TSSUTEXT
TITLE FOR REPORT (40 CHAR. MAX)
===>
(DEFAULT IS "SPECIAL REPORT")
ACID TO REPORT ON            ===>
(DEFAULT IS ALL ACIDS)
NUMBER OF PRIOR DAYS TO REPORT ON  ===>
(MAX 30 - DEFAULT IS 5)

```

Figure 22. ASO BATCH - TSSUTEXT Screen

Complete the fields as described:

Destination Information *conditional field*

Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.

Route *conditional field*

Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.

Message Class *conditional field*

Data is generated from the default parameters previously set-up **or** may be modified for the execution of this Job only.

Output Report To Dataset (Y/N)

optional, alpha; 1 position

Key in **Y** (yes) if you want the output report to go to dataset or **N** (no) if you do not want the output report to go to dataset. The system defaults to **N**.

Title For Report (40 Char. Max)

optional, alphanumeric; 40 positions max.

Key in the desired report title. If left blank, the system defaults to *Special Report*.

ACID To Report On

optional, alphanumeric; 8 positions max.

Key in the specific *user ID* you want to report on. If left blank, the system defaults to all *ACIDs* within your administrative scope of authority.

Number Of Prior Days To Report On

optional, numeric; 2 positions max.

Key in the number of prior days to report on. A maximum of 30 days may be entered. If left blank, the system defaults to 5 days.

When all applicable fields are completed, press **[Enter]**.

Output

Output is Option 10 on the ASO Batch Options Menu (**Figure 7**). This option is used to view/print output.

To select this option, key in **10** at the Option prompt. Press **[Enter]**.

The ASO Outlist Utility screen (**Figure 23**) is displayed.

```

----- ASO OUTLIST UTILITY ----- REL 1.0

OPTION  ==>

      L      - LIST JOB NAMES
      D      - DELETE JOB OUTPUT
      R      - REQUEUE JOB OUTPUT TO A NEW OUTPUT CLASS
      BLANK  - DISPLAY JOB OUTPUT

FOR JOB TO BE SELECTED:
  JOBNAME ==>
  JOBID   ==>

FOR JOB TO BE REQUEUED:
  NEW OUTPUT CLASS ==>

```

Figure 23. ASO Outlist Utility Screen

Below is a brief description of options available on the ASO Outlist Utility screen:

- L** - List Job Names
- D** - Delete Job Output
- R** - Requeue Job Output to a New Output Class
- BLANK** - Display Job Output

Complete the fields as described:

**For Job To Be Selected:
(JOBNAME)** *optional, alphanumeric field; 8 positions max.*
Key in the applicable JOBNAME.

**For Job To Be Selected:
(JOBID)** *optional, alphanumeric; 8 positions max.*
Key in the applicable JOBID.

For Job To Be Requeued: *optional, alpha; 1 position max. (A-Z or 7-9).*
Key in the applicable output class for your printer (i.e., **A**). Blank will requeue to your default output destination.

When all applicable fields are completed, press **[Enter]**.

Tutorial

Tutorial is Option T on the ASO Batch Options Menu (**Figure 7**). This option is used to display ISPF Help information.

To select this option, key in **T** at the Option prompt. Press **[Enter]**.

The ISPF Tutorial screen (**Figure 24**) is displayed. This screen is used for displaying ISPF Help information.

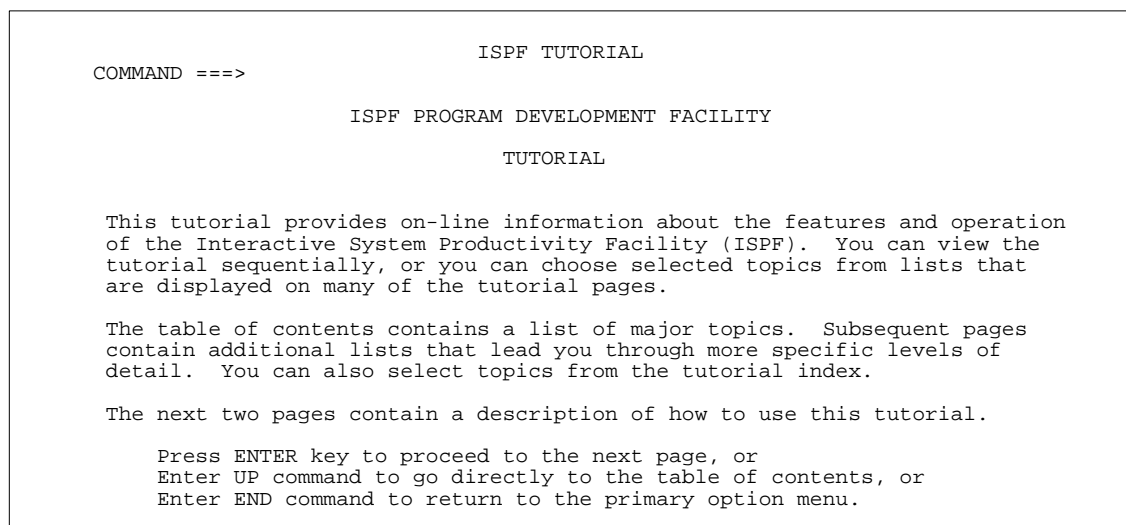


Figure 24. ISPF Tutorial Screen

Functions

Functions is Option 1 on the ASO Primary Option Menu (**Figure 5**). This menu is used to perform online commands.

To select this option, key in **1** at the Option prompt. Press **[Enter]**.

The ASO Functions Options Menu (**Figure 25**) is displayed.

```

----- ASO FUNCTIONS OPTIONS MENU ----- REL 1.0

OPTION  ===>

      0 LOCK          - LOCK YOUR TERMINAL
      1 UNLOCK        - UNLOCK YOUR TERMINAL
      2 WHO AM I      - DISPLAY INFO. ABOUT YOUR USERID/CURRENT SESSION
      3 ADD SUSPEND   - ADD SUSPEND ATTRIBUTE TO A USER
      4 REM SUSPEND   - REMOVE SUSPEND ATTRIBUTE FROM A USER
      5 REM SUSPEND & - REMOVE SUSPEND ATTRIBUTE FROM A USER
        REP PASSWORD - AND REPLACE THE PASSWORD
      6 REP PASSWORD  - REPLACE A USER'S PASSWORD
      7 TSSLIST       - LIST INFORMATION FOR AN ACID
      8 AMATRIX       - DETERMINE WHAT PROFILE FITS YOUR ACCESS REQUEST

      T TUTORIAL      - DISPLAY ISPF HELP INFORMATION
      X EXIT          - LEAVE ASO SECURITY FUNCTIONS

      HIT PF3 TO RETURN TO ASO PRIMARY OPTION MENU

```

Figure 25. ASO Functions Options Menu

To select an option, key in the selection **number** or **letter** at the Option prompt. Press **[Enter]**.

Below is a brief description of each option:

- 0** [LOCK](#) - Used to lock your terminal.
- 1** [UNLOCK](#) - Used to unlock your terminal.
- 2** [WHOAMI](#) - Used to display information about your user ID/current session.
- 3** [ADD SUSPEND](#) - Used to add suspend attribute to a user.
- 4** [REM SUSPEND](#) - Used to remove suspended attributes from a user.
- 5** [REM SUSPEND & REP PASSWORD](#) - Used to remove suspended attributes from a user and replace the password.
- 6** [REP PASSWORD](#) - Used to replace a user's password.
- 7** [TSSLIST](#) - Used to list information for an ACID.
- 8** [AMATRIX](#) - Used to determine what profile fits your access request.
- T** [TUTORIAL](#) - Provides the ISPF Tutorial screen used for displaying ISPF Help information.

X [EXIT](#) - Used to exit ASO security functions. Instructions to exit at any screen are provided in [Sign-Off](#) under **System Access**.

Lock

Lock is Option 0 on the ASO Functions Options Menu (**Figure 25**). This option is used to lock your terminal.

To select this option, key in **0** at the Option prompt. Press **[Enter]**.

A message near the bottom of the ASO Functions Options Menu is displayed informing you that your terminal is *locked* and the system displays *Function Successful*. Pressing **[Enter]** displays This Terminal Is Locked screen (**Figure 26**).

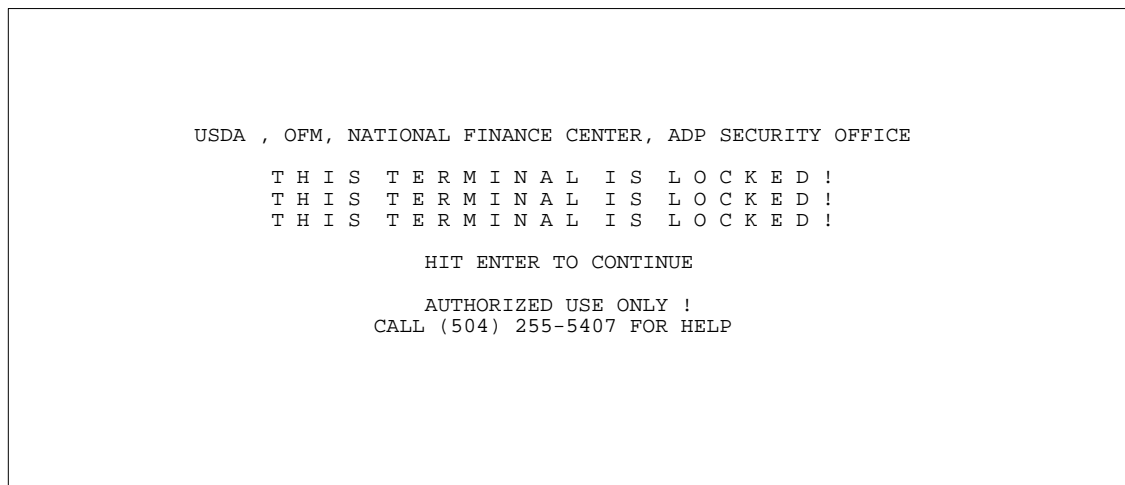


Figure 26. This Terminal Is Locked Screen

Unlock

Unlock is Option 1 on the ASO Functions Options Menu (**Figure 25**). This option is used to unlock your terminal.

To select this option, key in **1** at the Option prompt. Press **[Enter]**.

A screen is displayed asking for your password, key in your password and press **[Enter]**, the system displays the message that your terminal is now *unlocked*.

WHOAMI

WHOAMI is Option 2 on the ASO Functions Options Menu (**Figure 25**). This option is used to display information about an individual user ID/current session.

To select this option, key in **2** at the Option prompt. Press **[Enter]**.

The WHOAMI screen (**Figure 27**) is displayed.

```

DATE (XX/XX/XX)  TIME (XX:XX:XX)

YOU ARE RUNNING ON THE SYSB PROCESSOR

YOUR USERID IS.....NFXXX
YOUR PREFIX IS.....NFXXX
YOUR PROC NAME IS.....SECURE

TSS0303I ACIDNAME(NFXXX    ) TYPE(DCA ) MODE(FAIL    ) ADSP
TSS0303I FACILITY(TSO      ) TERMINAL(MULTTEST) LOCKTIME(000)
TSS0303I SYSTEMID(SYSB    ) LOG(ACCESS,SMF,MSG)
TSS0303I INSTDATA(REVISING PROCEDURE TO THE ASO PANEL)
TSS0300I WHOAMI      FUNCTION SUCCESSFUL
***

```

Figure 27. WHOAMI Screen

The screen displays the system processor you are running on, your user ID, your prefix, your proc name. It also lists the other secondary information regarding your user ID. At the bottom of the screen, the system displays the message *Function Successful*.

Add Suspend

Add Suspend is Option 3 on the ASO Functions Options Menu (**Figure 25**). This option is used to add suspended attributes to a user ID.

To select this option, key in **3** at the Option prompt. Press **[Enter]**.

The ASO Function - Add Suspend screen (**Figure 28**) is displayed.

```

-----
ASO FUNCTION - ADD SUSPEND                                REL 1.0
      USERID TO SUSPEND   ===>
-----
HIT ENTER TO CONTINUE  OR  PF3 TO CANCEL

```

Figure 28. ASO Function - Add Suspend Screen

Complete the field as described:

User ID To Suspend

required, alphanumeric; 8 positions max.

Key in the user ID of the user that will be suspended. Press **[Enter]**.

A suspended user identity screen (**Figure 29**) is displayed with a message that this person is *about to be suspended*. Is this correct? (Y/N)==>, key in **Y** (yes) to suspend the user and his/her user ID. Press **[Enter]**. Data is displayed on the screen (**Figure 29**) which describes the identity of the user that has been suspended.

```

USER ==> NFC User (NFXXX) ABOUT TO BE SUSPENDED

IS THIS CORRECT? (Y/N) ==> y


ACCESSORID = NFXXX      NAME      = NFC USER
TYPE       = USER      SIZE      =      256  BYTES
CREATED    = XX/XX/XX   LAST MOD  = XX/XX/XX  XX:XX
PROFILES   = N04SYS2F
ATTRIBUTES = NOATS
LAST USED  = XX/XX/XX   10:07 CPU(SYSSA) FAC(TSO   ) COUNT (14620)

TSS0300I LIST      FUNCTION SUCCESSFUL

USER NFXXX (NFC User) HAS BEEN SUSPENDED!

```

Figure 29. Suspended User Identity Screen

Press **[PF3]** twice to return to the ASO Functions Option Menu (**Figure 25**).

REM Suspend

REM Suspend is Option 4 on the ASO Functions Options Menu (**Figure 25**). This option is used to remove a suspended attribute from a user ID.

To select this option, key in **4** at the Option prompt. Press **[Enter]**.

The ASO Function - REM Suspend screen (**Figure 30**) is displayed.

```

-----
ASO FUNCTION - REM SUSPEND                                REL 1.0
  USERID TO UNSUSPEND  ==>
-----
HIT ENTER TO CONTINUE OR PF3 TO CANCEL

```

Figure 30. ASO Function - REM SUSPEND Screen

Complete the field as described:

User ID To Unsuspend *required, alphanumeric; 8 positions max.*

Key in the user ID to remove the suspended ID. Press **[Enter]**.

A remove suspended screen (**Figure 31**) is displayed with a message that this person is *about to be unsuspended*. Is this correct? (Y/N) ==>, key in **Y** (yes) to remove the suspended user and his/her user ID. Press **[Enter]**. Data is displayed on the screen (**Figure 31**) which describes the identity of the user that has been unsuspended.

```

USER ==> NFC User (NFXXX) ABOUT TO BE UNSUSPENDED

IS THIS CORRECT? (Y/N) ==> y

ACCESSORID = NFXXX      NAME      = NFC USER
TYPE        = USER      SIZE      = 256  BYTES
CREATED     = XX/XX/XX   LAST MOD  = XX/XX/XX  XX:XX
PROFILES    = N04SYS2F
ATTRIBUTES  = NOATS
LAST USED   = XX/XX/XX   10:07 CPU(SYSSA) FAC(TSO  ) COUNT (14620)

TSS0300I LIST      FUNCTION SUCCESSFUL

USER NFXXX (NFC User) HAS BEEN UNSUSPENDED!

```

Figure 31. Unsuspended User Identity Screen

Press **[PF3]** twice to return to the ASO Functions Option Menu (**Figure 25**).

REM Suspend & REP Password

REM Suspend & REP Password is Option 5 on the ASO Functions Options Menu (**Figure 25**). This option is used to remove suspended attributes from a user ID and replace the password.

To select this option, key in **5** at the Option prompt. Press **[Enter]**.

The ASO Function - REM Suspend & REP Password screen (**Figure 32**) is displayed.

```

-----
ASO FUNCTION - REM SUSPEND & REP PASSWORD                                REL 1.0
USERID      ==>
NEW PASSWORD ==>

NOTE: NEW PASSWORD WILL EXPIRE IMMEDIATELY AND HAS A 35 DAY
      EXPIRATION INTERVAL
-----
HIT ENTER TO CONTINUE OR PF3 TO CANCEL

```

Figure 32. ASO Function - REM SUSPEND & REP PASSWORD Screen

Complete the fields as described:

User ID

required, alphanumeric; 8 positions max.

Key in the user ID of the person having the suspended attributes removed.

New Password

required, alphanumeric; 8 positions max.

Key in the new password that replaces the suspended password. Press **[Enter]**.

Note: The new password will expire immediately and the user must establish his/her own password which has a 35 day expiration interval. Does not apply to T&A transmission ACIDS suffixed by X e.g., CA002X.

A remove suspend and replace password screen (**Figure 33**) is displayed with a message that this person is *about to be unsuspended and have password changed*. Is this correct? (Y/N) ==>, key in **Y** (yes) to remove suspend and replace the password. Press **[Enter]**. Data is displayed on the screen (**Figure 33**) which describes the identity of the user that has been unsuspended and their password changed.

```

USER ==> NFC User (NFXXX) ABOUT TO BE UNSUSPENDED AND
        HAVE PASSWORD CHANGED

IS THIS CORRECT? (Y/N) ==> y

ACCESSORID = NFXXX      NAME      = NFC USER
TYPE       = USER      SIZE      =      256  BYTES
CREATED    = XX/XX/XX   LAST MOD  = XX/XX/XX  XX:XX
PROFILES   = N04SYS2F
ATTRIBUTES = NOATS
LAST USED  = XX/XX/XX   10:07 CPU(SYSSA) FAC(TSO   ) COUNT (14620)

TSS0300I LIST      FUNCTION SUCCESSFUL

USER NFXXX (NFC User) HAS BEEN UNSUSPENDED AND PASSWORD
HAS BEEN CHANGED
***
  
```

Figure 33. Remove Suspend And Replace Password For User Screen

Press **[PF3]** twice to return to the ASO Functions Option Menu (**Figure 25**).

REP Password

REP Password is Option 6 on the ASO Functions Options Menu (**Figure 25**). This option is used to replace a user's password.

To select this option, key in **6** at the Option prompt. Press **[Enter]**.

The ASO Function - REM Suspend & REP Password screen (**Figure 32**) is displayed. Complete the fields as described for option 5. Press **[Enter]**. A REM Suspend & REP

Password screen (**Figure**) is displayed. Response is the same as described for REM Suspend & REP Password screen. Press **[PF3]** twice to return to the ASO Functions Options Menu (**Figure 25**).

TSSLIST

TSSLIST is Option 7 on the ASO Functions Options Menu (**Figure 25**). This option is used to list information for an ACID.

To select this option, key in **7** at the Option prompt. Press **[Enter]**.

The ASO List - TSSLIST screen (**Figure 34**) is displayed.

ASO LIST - TSSLIST

REL 1.0

ACID ==>

DATA ==> ALL

DATA VALUES: (DEFAULT 'BASIC')

ACIDS, ADMIN, ALL, BASIC, CICS, INSTDATA, LCF,

NAMES, PASSWORD, RESOURCE, SOURCE, XAUTH

DIVISION ==> (VALID FOR ZCAS ONLY)

DEPT ==> (VALID FOR ZCAS ONLY)

TYPE ==>

HIT ENTER TO CONTINUE OR PF3 TO CANCEL

Figure 34. ASO List - TSSLIST Screen

Complete the fields as described:

- ACID

required, alphanumeric; 8 positions max.

Key in the user ID (ACID) concerning the information you want listed.
- DATA

optional, alpha; 8 positions max.

Key in the data values e.g., **ACIDS, ADMIN, ALL, BASIC, PROF, CICS, INSTDATA, LCF, NAMES, RESOURCE, SOURCE, XAUTH**. The system defaults to **ALL**.
- Division

optional, alpha; 8 positions max.

Key in the division (valid for ZCAS only) for an ACID.
- Dept

optional, alpha; 8 positions max.

Key in the department (valid for VCAS only) for an ACID.

Type

optional, alphanumeric; 8 positions max.

Key in the type ACID (user ID) concerning the information you want listed.
Press **[Enter]**.

Amatrix

Amatrix is Option 8 on the ASO Functions Options Menu (**Figure 25**). This option is used to determine the appropriate profile to fit your access request.

To select this option, key in **8** at the Option prompt. Press **[Enter]**

The ASO Function - Amatrix screen (**Figure 35**) is displayed.

```

-----
ASO FUNCTION - AMATRIX                                REL 1.0
VIEW MEMBER LIST FIRST? (Y OR N)      ===>
ORGANIZATION FOR WHICH YOU WANT THE
SECURITY MATRIX LISTED                ===>
-----
HIT ENTER TO CONTINUE OR PF3 TO CANCEL

```

Figure 35. ASO Functions - AMATRIX Screen

Complete the fields as described:

View Member List First? (Y Or N)

conditional, alpha field; 1 position

Key in **Y** (yes) if you want to view the member list first, press **[Enter]**. A listing of possible member names is displayed. If you do not want to view the member list first, key in **N** (no).

Organization For Which You Want The Security Matrix Listed

conditional, alpha; 8 positions max.

Key in the organization for which you want the security matrix listed, when **N** (no) is keyed in block 1.

Note: This field is **not** required when you key in **Y** (yes) in block 1. Press **[Enter]**.

Tutorial

Tutorial is Option T on the ASO Functions Options Menu (**Figure 25**). This option is used to display ISPF Help information.

To select this option, key in **T** at the Option prompt. Press **[Enter]**.

The ISPF Tutorial screen (**Figure 36**) is displayed. This screen is used for displaying ISPF Help information.

```
COMMAND ==>                                ISPF TUTORIAL
                                           ISPF PROGRAM DEVELOPMENT FACILITY
                                           TUTORIAL

This tutorial provides on-line information about the features and
operation of the ISPF program development facility (ISPF/PDF). You can
view the tutorial sequentially, or you can choose selected topics from
lists that are displayed on many of the tutorial pages.

The table of contents contains a list of major topics. Subsequent pages
contain additional lists that lead you through more specific levels of
detail. You can also select topics from the tutorial index.

Press ENTER key to proceed to the next page, or
Enter UP command to go directly to the table of contents, or
Enter END command to return to the primary option menu.
```

Figure 36. ISPF Tutorial Screen

Lists

Lists is Option 2 on the ASO Primary Option Menu (**Figure 5**). This option is used to perform online list commands.

To select this option, key in **2** at the Option prompt. Press **[Enter]**.

The ASO List Options Menu (**Figure 37**) is displayed.

```

----- ASO LIST OPTIONS MENU ----- REL 1.0
OPTION  ===>

0  TSSLIST      -  LIST INFORMATION FOR ACID
1  ACCESS       -  LIST SECURITY SPECS FOR AN APPLICATION
2  MATRIX       -  LIST THE SECURITY MATRIX FOR YOUR ORGANIZATION
3  OFFICER      -  LIST CLIENT SECURITY OFFICER PHONE NUMBERS
4  PRINT        -  PRINT ACCESS, MATRIX, OR OFFICER LISTING

T  TUTORIAL     -  DISPLAY ISPF HELP INFORMATION
X  EXIT         -  LEAVE ASO SECURITY FUNCTIONS

HIT PF3 TO RETURN TO ASO PRIMARY OPTION MENU

```

Figure 37. ASO List Options Menu

Below is a brief description of each option:

- 0** [TSSLIST](#). Used to list information for ACIDs.
- 1** [ACCESS](#). Used to list security specs for an application.
- 2** [MATRIX](#). Used to list the security matrix for your organization.
- 3** [OFFICER](#). Used to list client security officer phone numbers, addresses, etc.
- 4** [PRINT](#). Used to print access, matrix, or officer listings.
- T** [TUTORIAL](#). Provides the ISPF Tutorial screen used for displaying ISPF Help information.
- X** [EXIT](#). Used to exit ASO security functions. Instructions to exit at any screen are provided in Sign-Off under System Access.

TSSLIST

TSSLIST is Option 0 on the ASO List Options Menu (**Figure 37**). This option is used to list information for an ACID.

To select this option, key in **0** at the Option prompt. Press **[Enter]**.

The ASO List - TSSLIST screen (**Figure 34**) is displayed. Complete the fields as described for fields 1 through 5.

Access

Access is Option 1 on the ASO List Options Menu (**Figure 37**). This option is used to list security specs for an application.

To select this option, key in **1** at the Option prompt. Press **[Enter]**.

The ASO List - Access screen (**Figure 38**) is displayed.

ASO LIST - ACCESSREL 1.0

VIEW MEMBER LIST FIRST? (Y OR N)====>

APPLICATION FOR WHICH YOU WANT SECURITY
SPECIFICATIONS LISTED====>

HIT ENTER TO CONTINUE OR PF3 TO CANCEL

Figure 38. ASO List - ACCESS Screen

Complete the fields as described:

**View Member List First?
(Y Or N)**

conditional, alpha; 1 position

Key in **Y** (yes) if you want to view the member list first, press **[Enter]**. A listing of possible member names is displayed. If you do not want to view the member list first, key in **N** (no).

**Application For Which
You Want Security
Specifications Listed**

conditional, alpha; 8 positions max.

Key in the application for which you want security specifications listed, when **N** (no) is keyed in block 1.

Note: This field is **not** required when you key in **Y** (yes) in block 1. Press **[Enter]**.

Matrix

Matrix is Option 2 on the ASO List Options Menu (**Figure 37**). This option is used to list the security matrix for your organization.

To select this option, key in **2** at the Option prompt. Press **[Enter]**. The ASO List - Matrix screen (**Figure 39**) is displayed.

```
-----
ASO LIST  - MATRIX                                REL 1.0
VIEW MEMBER LIST FIRST?  (Y OR N)      ===>
ORGANIZATION FOR WHICH YOU WANT THE
SECURITY MATRIX LISTED      ===>
-----
HIT ENTER TO CONTINUE  OR  PF3 TO CANCEL
```

Figure 39. ASO List - Matrix Screen

Complete the fields as described:

**View Member List First?
(Y Or N)**

conditional, alpha; 1 position

Key in **Y** (yes) if you want to view the member list first, press **[Enter]**. A listing of possible member names is displayed. If you do not want to view the member list first, key in **N** (no).

**Organization For Which
You Want The Security
Matrix Listed**

conditional, alpha; 8 positions max.

Key in the organization for which you want the security matrix listed, when **N** (no) is keyed in block 1.

Note: This field is **not** required when you key in **Y** (yes) in block 1. Press **[Enter]**.

Officer

Officer is Option 3 on the ASO List Options Menu (**Figure 37**). This option is used to list client security officer phone numbers addresses, etc.

To select this option, key in **3** at the Option prompt. Press **[Enter]**.

The ASO List - Officer screen (**Figure 40**) is displayed.

```
-----
ASO LIST  - OFFICER                                     REL 1.0

VIEW MEMBER LIST FIRST?  (Y OR N)          ===>

ORGANIZATION FOR WHICH YOU WANT SECURITY
OFFICER NAME AND PHONE NUMBERS LISTED     ===>
-----
HIT ENTER TO CONTINUE  OR  PF3 TO CANCEL
```

Figure 40. ASO List - Officer Screen

Complete the fields as described:

**View Member List First?
(Y Or N)**

conditional, alpha; 1 position

Key in **Y** (yes) if you want to view the member list first, press **[Enter]**. A listing of possible member names is displayed. If you do not want to view the member list first, key in **N** (no).

**Organization For Which
You Want The Security
Officer Name And Phone
Numbers Listed**

conditional, alpha; 30 positions max.

Key in the organization for which you want security officer name and phone numbers listed, when **N** (no) is keyed in block 1.

Note: This field is **not** required when you key in **Y** (yes) in block 1. Press **[Enter]**.

Print

Print is Option 4 on the ASO List Options Menu (**Figure 37**). This option is used to print access, matrix, or officer listings. To select this option, key in **4** at the Option prompt. Press **[Enter]**.

The ASO List - Print screen (**Figure 41**) is displayed.

```
-----
ASO LIST  - PRINT                                REL 1.0

VIEW MEMBER LIST FIRST?  (Y OR N)                ===>

VIEW/PRINT ACCESS LIST(A),
MATRIX LIST(M), OR OFFICER LIST(O)?
ENTER A, M, OR O AS APPROPRIATE                  ===>

ACCESS, MATRIX, OR OFFICER MEMBER TO PRINT      ===>
-----
HIT ENTER TO CONTINUE OR PF3 TO CANCEL
```

Figure 41. ASO List - Print Screen

**View Member List First?
(Y Or N)**

required, alpha; 1 position

Key in **Y** (yes) if you want to view the member list first, press **[Enter]**. A listing of possible member names is displayed. If you do not want to view the member list first, key in **N** (no).

**View/Print Access List
(A), Matrix List (M), Or
Officer List (O)?**

conditional, alpha; 1 position

Key in the appropriate letter **A**, **M**, or **O** to view/print.

**Access, Matrix, Or
Officer Member To Print**

conditional, alphanumeric; 8 positions max.

Key in either **Access**, **Matrix**, or **Officer Member** to print.

Note: This field is **not** required when you key in **Y** (yes) in block 1. Press **[Enter]**.

Tutorial

Tutorial is Option T on the ASO List Options Menu (**Figure 37**). This option is used to display ISPF Help information.

To select this option, key in **T** at the Option prompt. Press **[Enter]**.

The ISPF Tutorial screen (**Figure 42**) is displayed. This screen is used for displaying ISPF Help information.

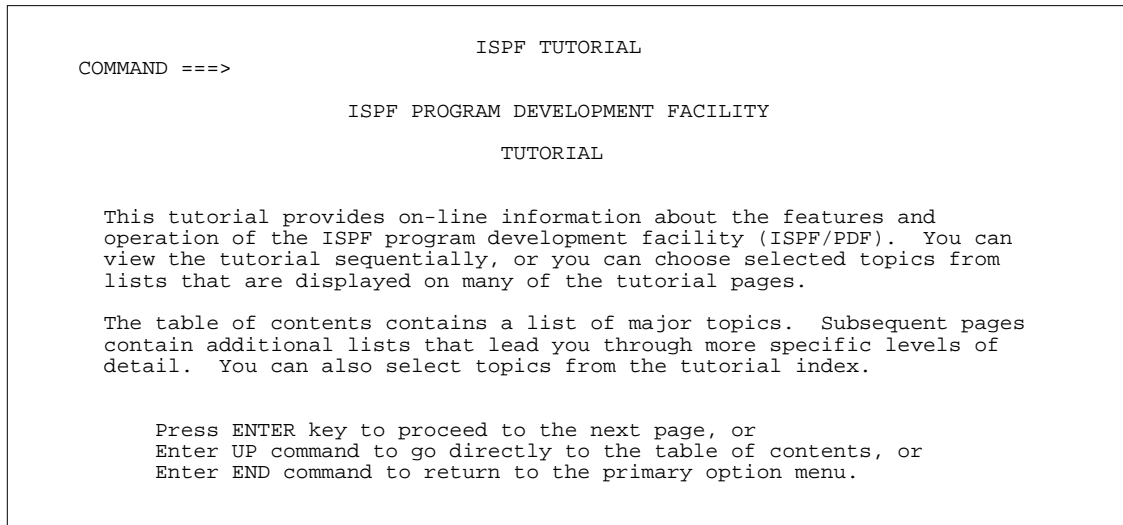


Figure 42. ISPF Tutorial Screen

Glossary

Glossary is Option G on the ASO Primary Option Menu (**Figure 5**). This option is used to provide a glossary of terms used in the Security Access system.

To select this option, key in **G** at the Option prompt. Press **[Enter]**.

The ASO Panels Glossary menu (**Figure 43**) is displayed.

```

*****
                        ASO PANELS GLOSSARY
*****
ENTER ANY CHARACTER NEXT TO A FIELD(S) TO SELECT

. ACID                . BATCH                . CICS
. CPU                 . ERROR MESSAGE    . FACILITY
. GENERIC PREFIX      . JCL              . MASKING
. MODE                . MVS              . OWNERSHIP
. PASSWORD            . PERMISSIONS      . PREFIXING
. PROFILES            . RESOURCE         . SECURITY ADMIN
. TSO                 . USERID          . VIOLATION

HIT ENTER TO CONTINUE, PF3 TO RETURN TO PREVIOUS MENU
*****

```

Figure 43. ASO Panels Glossary Menu

To select a word from the glossary, place any character next to the left side of the term or terms and press **[Enter]**.

Below is a brief description of terms or words used in the Security Access system:

- **ACID.** A unique character-string identifier of a user's security record.
- **BATCH.** A method of processing large amounts of data at one time.
- **CICS.** An acronym for Customer Information Control System.
- **CPU.** An acronym for Central Processing Unit.
- **ERROR MESSAGE.** A system response that is displayed to inform the user that the entered transaction was not valid.
- **FACILITY.** An MVS (Multiple Virtual System) subsystem that processes work on behalf of users and jobs, e.g., TSO, CICS, IDMS, BATCH, etc.
- **GENERAL PREFIX.** A shorthand way to specify a number of similarly-named resources in the same resource class.
- **JCL.** An acronym for Job Control Language.
- **MASKING.** A technique that can be used to reduce the number of definitions needed to be defined to CA-Top Secret.

- **MODE.** The security implementation stage that determines the manner in which CA-Top Secret processes resource access requests. The four modes are: FAIL, WARN, IMPLEMENT, and DORMANT.
- **MVS.** An acronym for Multiple Virtual System.
- **OWNERSHIP.** Within the CA-Top Secret database structure, all resources must be *owned* before they can be used and secured.
- **PASSWORD.** A unique string of characters associated with a particular user ACID. Signon cannot be successful if an incorrect password is supplied.
- **PERMISSIONS.** The process that makes an owned resource available to other users in a controlled manner.
- **PREFIXING.** Allows a group of similar resources of the same type to be defined to CA-Top Secret simultaneously.
- **PROFILES.** A special ACID type within CA-Top Secret that allows a group of users, performing the same job function, to be permitted the same group of resources.
- **RESOURCE.** Items or functions protected by CA-Top Secret such as, a dataset, program, transaction, etc.
- **SECURITY ADMINISTRATOR.** A person designated and authorized to grant users permission to access resources.
- **TSO.** An acronym for Time Sharing Option.
- **user ID.** An ACID assigned to an individual. The user ID is used to signon to the system.
- **VIOLATION.** An attempt to access a resource that has not been authorized.

Messages

Messages is Option M on the ASO Primary Option Menu (**Figure 5**). This option is used to display the common TSS messages.

To select this option, key in **M** at the Option prompt. Press **[Enter]**.

The ASO Panels TSS Messages menu (**Figure 44**) is displayed.

```

*****
                        ASO PANELS TSS MESSAGES
*****
ENTER ANY CHARACTER NEXT TO A FIELD(S) TO SELECT

. TSS7000I          . TSS7011A          . TSS7101E
. TSS7110E          . TSS7141E          . TSS7143E
. TSS7160E          . TSS7172E          . TSS7221E
. TSS7227E          .                  .

HIT ENTER TO CONTINUE,  PF3 TO RETURN TO PREVIOUS MENU
*****

```

Figure 44. ASO Panels TSS Messages Menu

Below is a brief description of the TSS Messages:

- **TSS7000I.** *ACID last-used date time System=ID Facility=facility.* This message appears when you logon and also at the beginning of your BATCH jobs. It informs you as to when you last used the system, etc.
- **TSS7011A.** *Please enter your New password.* This message appears when your CA-Top Secret password has expired and you must enter a new password to continue your logon.
- **TSS7101E.** *Password is incorrect.* This message appears when the password you supplied for the ACID is invalid. Access to the system will not be allowed until the correct combination of ACID and password is supplied.
- **TSS7110E.** *Password has expired. New password missing.* This message appears when your CA-Top Secret password has expired and you must enter a new password to continue your logon.
- **TSS7141E.** *Use of Accessor ID suspended.* This message appears when the use of your ACID (user ID) has been revoked for one or more of the following reasons:
 1. The Suspend attribute was added to your ACID (user ID) by your Security Officer.
 2. You Suspended yourself by incorrectly specifying your password 5 times when attempting to logon to the system.

3. The system automatically suspended your ACID (user ID) because you had not used your user ID for an extended period of time.
- **TSS7143E.** *ACID has been inactive too long.* This message appears when your ACID (user ID) has exceeded an inactivity threshold as set by the CA-Top Secret security software. Inactivity is measured from the last time the ACID's password was changed to the current date.
 - **TSS7160E.** *Facility not authorized for your use.* This message appears when you do not have access to the facility (i.e., TSO, BATCH, CICSxx, IDMSxx, etc.).
 - **TSS7172E.** *Your ACID is already in use on a terminal.* This message appears when your ACID (user ID) is already signed on to the system at the terminal specified.
 - **TSS7221E.** *Dataset not accessible - dataset name.* This message appears when you do not have the security access required to access the dataset.
 - **TSS7227E.** *Access not granted to dataset - dataset name.* This message appears when you do not have the required access level to access the dataset.

History

History is Option H on the ASO Primary Option Menu (**Figure 5**). This option is used to retrieve a history of ASO bulletin board messages.

To select this option, key in **H** at the Option prompt. Press **[Enter]**.

The ASOMSG - ASO Bulletin Board Message History Display Utility screen (**Figure 45**) is displayed.

```

-----
ASOMSG - ASO BULLETIN BOARD MESSAGE HISTORY DISPLAY UTILITY          REL 1.0

VIEW LIST OF OLD MESSAGES FIRST? (Y OR N) ==>

MESSAGE YOU WANT DISPLAYED          ==>

PLEASE NOTE:
(1)  THE MESSAGE NAMES ARE IN THE FORMAT  X YY MM DD S WHERE;
      X   = THE LITERAL "M"
      YY  = THE YEAR THE MESSAGE WAS CREATED
      MM  = THE MONTH THE MESSAGE WAS CREATED
      DD  = THE DAY THE MESSAGE WAS CREATED
      S   = A SUFFIX INDICATING MULTIPLE MESSAGES FOR A GIVEN DATE

(2)  YOU WILL BE PRESENTED WITH A "STATIC" DISPLAY OF A MESSAGE.
      MESSAGE TEXT INDICATING "PF3 TO GO BACK", ETC. HAS NO EFFECT.
      REFER TO THE MESSAGE BELOW TO NAVIGATE USING THE ASOMSG UTILITY.
-----
HIT ENTER TO CONTINUE  OR  PF3 TO CANCEL
  
```

Figure 45. ASO Bulletin Board Message History Display Utility Screen

Complete the fields as described:

View List Of Old

Messages First? (Y Or N) *conditional, alpha; 1 position*

Key in **Y** (yes) if you want to view old messages first or key in **N** (no) if you do not want to view the most current messages.

Message You Want Displayed

conditional, alpha; 15 positions max.

Key in the applicable message date in the **YY MM DD** format, and key in **S** for a suffix indicating multiple messages for a given date, when **N** is keyed in block 1. Press **[Enter]**.

Standards

Standards is Option S on the ASO Primary Option Menu (**Figure 5**). This option is used to describe the standards for password management and user access authorization.

To select this option, key in **S** at the Option Prompt. Press **[Enter]**.

The BROWSE -- NFCPSECU.SUPPORT.STANDARD screen (**Figure 46**) is displayed.

```
BROWSE      NFCPSECU.SUPPORT.STANDARD                      Line 00000000 Col 001 080
COMMAND ==>                                           SCROLL ==> PAGE
***** TOP OF DATA *****
-----
Following are the NFC standards for password management and
user access authorization.  You may scroll through this dataset by
pressing {PF7} to scroll up or {PF8} to scroll down.  Use {PF3} to
return to the ASO panels
-----

                                USER ACCESS AUTHORIZATION

1.0      General

Access to NFC will only be provided for only those individuals requiring
access to perform an assigned job function.  All system users will be
assigned a unique user identification (userid) that will be used for
access to all NFC system resources.
```

Figure 46. BROWSE -- NFCPSECU.SUPPORT.STANDARD Screen

The Standard screen displays the NFC standards for password management and user access authorization. You may scroll through this dataset by pressing **[PF8]** to scroll down to the next screen or **[PF7]** to scroll up to the previous screen. Press **[PF3]** to return to the ASO Primary Option Menu.

Tutorial

Tutorial is Option T on the ASO Primary Option Menu (**Figure 5**). This option is used to display ISPF Help information.

To select this option, key in **T** at the Option prompt. Press **[Enter]**.

The ISPF Tutorial screen (**Figure 47**) is displayed. This screen is used for displaying ISPF Help information.

```
COMMAND ===>                                ISPF TUTORIAL

                                           ISPF PROGRAM DEVELOPMENT FACILITY

                                           TUTORIAL

This tutorial provides on-line information about the features and
operation of the ISPF program development facility (ISPF/PDF). You can
view the tutorial sequentially, or you can choose selected topics from
lists that are displayed on many of the tutorial pages.

The table of contents contains a list of major topics. Subsequent pages
contain additional lists that lead you through more specific levels of
detail. You can also select topics from the tutorial index.

Press ENTER key to proceed to the next page, or
Enter UP command to go directly to the table of contents, or
Enter END command to return to the primary option menu.
```

Figure 47. ISPF Tutorial Screen

Access To FFIS

This section provides the policies and procedures for controlling access to NFC's Foundation Financial Information System (FFIS). The policies and procedures are intended to provide reasonable assurance that only authorized individuals have access to FFIS and these individuals are able to perform those functions needed to accomplish their assigned duties. The following is the policy used by NFC and may be used as a model for other agencies.

Background

The Office of the Chief Financial Officer (OCFO) has led the USDA Financial Information System Vision and Strategy (FISVIS) project to provide the Department with a single financial information system. In December 1994, USDA awarded a contract to American Management Systems (AMS) to provide and assist in implementing FFIS. USDA processes data from over 40 entities, some of these entities are USDA agencies and others are cross-serviced agencies. Most of the data processed by USDA is sensitive in nature and must be protected from both internal and external unauthorized access. Specifically:

- Unauthorized users are **not** allowed on the NFC mainframes.
- Agencies are **not** allowed to view or query another agency's data.
- Within each agency varying levels of control are used to restrict access to the agency's data.

Requirements are met through several levels of control, which are outlined below:

- NFC employs two different security systems that work together to protect FFIS against unauthorized access, the mainframe computer security system and the FFIS security system.
- CA-Top Secret is a security software package used to control access to mainframe resources. The mainframe computer security system primarily protects FFIS against unauthorized offline access and provides general computer access protection. Additionally, the FFIS security system requires a specific logon to FFIS once access to the mainframe has been attained through the CA-Top Secret security package. Without the specific FFIS logon, online access to FFIS cannot be attained. When logged on, the FFIS security system controls which user has access and the degree of that access on an individual-by-individual basis. In the functionality of the FFIS baseline software, it is possible to enforce row-level security at two levels; (1) SEC1 and (2) SEC2.
- The FFIS structure provides a separate application image for each agency. Each application image consists of data that is owned by that agency with some reference data that is owned by OCFO. FFIS data resides in a database that is composed of DB2 data tables. Agencies are responsible for the control and integrity of tables that contain only their data. The OCFO is responsible for the control and integrity of data in tables that **do not** belong to a single agency.

Concept Of Security Operation

The highest level financial office at an agency will be the Office of Primary Responsibility (OPR). The OPR is the owner of the agency's financial data and is responsible for the security of FFIS data. The senior official of the OPR or their designee must accept the responsibility for the ownership, integrity, confidentiality, and availability of this data. The OPR also defines the security requirements for this data. One of the primary functions of the owner is to determine who will have access to this data and the type of access.

Each OPR may designate an Application Administrator with an accounting and financial background to manage the related FFIS data. The OPR's Application Administrator is accountable to the OPR and is responsible for approving the access requests for personnel needing access to their data. If an Application Administrator is designated, an alternate Application Administrator(s) should also be designated by the OPR.

The decision on how the internal security administration is controlled is based on what provides the correct level of security and services to agency users.

When establishing an agency's application image, NFC sets up the access for the person designated as the agency's Security Administrator. After the agency's Access Administrator is set up, he/she will be able to set up and maintain all subsequent FFIS access requests for the agency's application image.

Designated OCFO and NFC personnel will require access to each agency's application image to perform system-wide functions. NFC's Information Systems Security Officer (ISSO) sets up and maintains the specific security group for each agency's application image.

Procedure For Establishing And Defining Roles For FFIS Security

Each financial office with an FFIS data owner is responsible for designating one Application Administrator and their alternates.

Since the Application Administrators have a pivotal role in helping to ensure that FFIS is protected against unauthorized access, it is very important that the individuals selected to perform these functions are qualified. Individuals considered for the position of Application Administrator or an alternate, should have a strong accounting background and have clearly demonstrated:

- Integrity and a strong commitment to carry out their responsibilities dependably.
- Knowledge of their office's operation, personnel, and FFIS.
- An understanding of basic internal control concepts.
- Ability to determine the success of batch processing jobs.
- Ability to identify correct settings for tables that affect production of financial statements.
- A working knowledge of mainframe computer architecture, including the different parts (e.g., database, application, tablespace, etc.) in order to understand the impact of the decisions that are made.

All Application Administrators and their alternates **must** be formally designated in writing to NFC by their management. Any change in Application Administrators or their alternates **must also** be designated in writing. For individuals selected as Application Administrators or alternates, the information below **must** be provided to everyone in the financial office (so he/she will know who to send their access requests to) and to the Agency Security Administrator (so he/she will know who to accept access requests from):

- Name
- Address
- Telephone number
- Position
- Define if they will be the Application Administrator or an alternate.

Each agency currently will have or will designate one or more Information System Security Program Manager (ISSPM) or Agency Security Administrator. The Agency Security Administrator could also serve in the capacity of Security Administrator for the application. Departmental Regulation (DR) 3140 and Departmental Manual (DM) 3140-1 define the roles and responsibilities for the Information System Security Program Administrator.

The individual(s) selected to be the ISSO and deputy must possess and demonstrate the required knowledge, skills, and abilities necessary to competently perform Agency Security Administrator's function includes the knowledge of the Agency's organizational structure and FFIS operations (including the security features).

Note: The Agency Security Administrator and the deputy/alternate will be assigned separate user ID's and passwords. Neither will have the capability to enter, edit, update, or approve documents or the ability to add, change, or delete tables other than those directly related to performing the Agency Security Administrator functions in FFIS.

NFC's ISSO will only accept access requests from Agency Security Administrators. Therefore, when an Agency Security Administrator is designated, the agency must provide the name, user ID, telephone number, and effective date of the appointment to:

Information Systems Security Office
National Finance Center, USDA
P.O. Box 60000
New Orleans, LA 70160

Procedures For Acquiring FFIS Access

Each agency determines what level of management initiates the requests for FFIS access. The Application Administrator will **only** expect to authorize access requests from the management level that has been designated.

The authorized level of management should complete an FFIS Internal Security Access Request Form in accordance with the detailed instructions in Exhibit 1.

Submit the completed form to their Application Administrator for review and approval.

After examining the FFIS Internal Security Access Request Form for appropriateness, the Application Administrator will do one of the following:

- Approve the request with no changes.
- Approve the request with modifications (notifies the requester of the modifications).
- Disapprove the request (notifies the requester).

If there is any disagreement with the Application Administrator's decision, an appeal should be made to the owner of the data. The owner's decision will be **final**.

The requester should keep a copy of all approved FFIS Internal Security Access Request Forms on file for reference when requesting modifications to his/her access.

The Application Administrator sends the original approved FFIS Internal Security Access Request Form to the Agency Security Administrator.

The Agency Security Administrator ensures that the appropriate Application Administrator has approved the access and the range of the access is within the authority of the Application Administrator.

- If the potential user does not have an NFC user ID, the Agency Security Administrator submits a request to NFC to establish the required access.
- NFC notifies the Agency Security Administrator and the requester when the NFC user ID and access have been implemented.

The Agency Security Administrator implements appropriately prepared and authorized FFIS access requests.

The Agency Security Administrator informs the requester that his/her access has been implemented.

Procedures For Changes To FFIS Access

When an FFIS user access needs to be changed, follow the instructions below:

- The requester obtains an FFIS Internal Security Access Request Form and completes the form according to the detailed instructions provided in **Exhibit 1**. Because this request supersedes any existing requests, it **must** list all capabilities required. The request **cannot** be limited to only the new capabilities that will be added to the existing FFIS security profile, nor can it be limited to the capabilities that will be eliminated from the existing FFIS security profile.
- The requester submits the completed FFIS Internal Security Access Request Form to his/her Application Administrator.
- The Application Administrator reviews the form, approves and/or modifies or disapproves the request, notifies the requester about approval, modifications, or disapproval.
- If any disagreements with the Application Administrator's decision, an appeal should be made to the owner of the data. The data owner's decision will be **final**.

- The requester should keep a copy of all approved FFIS Internal Security Access Request Forms for reference when requesting modifications to a user's access within his/her scope of authority.
- The Application Administrator sends the original approved FFIS Internal Security Access Request Form to the Agency Security Administrator.
- The Agency Security Administrator ensures that the appropriate Application Administrator has approved the access and the scope of the access is within the authority of that Application Administrator.
- The Agency Security Administrator implements appropriately prepared and authorized FFIS access requests.
- The Agency Security Administrator informs the requester that his/her access has been modified.

Procedures For Requesting Deletion Of FFIS Access

When the user no longer needs an FFIS access, the request to delete FFIS access instructions follow:

- The requester obtains an FFIS Internal Security Access Request Form and completes the form according to the detailed instructions provided in [Exhibit 1](#).
- The requester submits the completed FFIS Internal Security Access Request Form to his/her Application Administrator.
- The Application Administrator reviews the form and submits it to the Agency Security Administrator for implementation. The Application Administrator can expedite deletions by telephone or electronic mail but a follow up of a hard copy of the request form **must** be provided. Requests for deletions by telephone or electronic mail **must** provide the name of the individual to be deleted including their NFC user ID and office.
- The Agency Security Administrator removes the FFIS access and notifies the requester of the deletion.
- The Agency Security Administrator notifies NFC of the deletion and NFC removes the Top Secret access to FFIS.

Note: When implementing deletions, the Agency Security Administrator should include access for other applications for that user, if applicable, and notify NFC. If the person is also losing **all** existing access for any reason, NFC should be notified.

Roles And Responsibilities

Agency Management will:

- Designate one or more Application Administrators.
- Describe what organization level(s) own and control FFIS data access.
- Appoint an Agency Security Administrator and/or deputy Agency Security Administrator in accordance with DR 3140-1, or appoint a Security Administrator with responsibilities limited to FFIS Security Officer.

- Resolve appeals of disapproved access requests.

Application Administrators will:

- Be responsible for reviewing access requests received to:
Provide reasonable assurance that access to FFIS is limited to authorized individuals and that individuals are **not** granted more privileges than they need to perform their properly assigned responsibilities.
Ensure that requested functions, coming from authorized requesters, are compatible with office needs and do not compromise the Agency's internal controls.
- Be responsible for ensuring proper establishment of:
Security group definitions and model security profiles using the FFIS Internal Security Access Request Form ([Exhibit 1](#)).
Security groups that can access each FFIS table name and document name using the FFIS Internal security Access Specification Form Form/Fort/Fors Table ([Exhibit 2](#)).
- Establish procedures regarding changes in personnel assignments for FFIS and inform the Agency Security Administrator regarding changes in personnel's need for access. Such changes include, but are not limited to, termination of employment and major changes in job responsibilities.
- Analyze the appropriateness of FFIS access. Application Administrators **must** read the access to FFIS profiles or TSS profiles for the organizational level applicable for this access purpose.
- **Never** provide any individual with FFIS capabilities that results in an individual having an excessive concentration of responsibilities. Concentrating too many responsibilities in the hands of one individual compromises the Agency's internal controls and unnecessarily increases the risk of errors and irregularities (fraud and abuse).
- **Not** allow certifying officers to enter or modify payment data, or to modify vendor file records to certified documents.
- **Not** allow individuals, having the ability to approve accounts receivable write-offs on FFIS, to also enter or modify accounts receivable transactions using FFIS.
- Control System Options Tables such as Disbursing Options Tables (DOPT).
- Coordinate the use of the application, identifying on and off times for demonstrations and batch jobs.
- Coordinate and authorize application backups and restores. The Application Administrator ensures that all backups and restores are accomplished only when it is acceptable to **all** users of the application.
- **Not** be responsible for performing security administration functions within the application.
- Ensure that the parameters required for batch jobs are correct and authorize execution of batch jobs. This includes, but it not limited to the following:
 - a. Nightly cycle (i.e., OFFCTL and RUNSPLT).

b. Monthly close.

c. Annual close.

- Coordinate maintenance and conformation activities with the FFIS technical personnel.
- Make decisions about application run errors and the resolution of those errors.
- Review results about batch activities to ensure consistency with expected results.

Agency Security Administrators will:

- Establish, monitor, and revise entries or data for controlling FFIS internal security, as required.
- Establish and revise policies and procedures for access to FFIS, as needed.
- Establish and revise internal policies and procedures for performing the Agency Security Administrator functions, as needed.
- Maintain the following FFIS security-related tables:

Security Table (STAB) is used to establish internal user ID's and assign them to security groups. It also is used to define the override and approval authorities for each user.

Format Definition Table (FORM) is used to assign security groups to application tables and documents. It also is used to set approval and override levels for application errors on documents.

Security Logging Table (SLOG) is where security errors are logged for review by the Application Administrator. This table tracks unauthorized attempts to access or process data.

User Identification Table (USID) indicates a user ID as active or inactive. Initial definition of a user ID on the STAB table defines a user to this table.

- Identify and notify the agency's management of any known weakness in the FFIS security process.
- Only accept and implement FFIS access requests approved by the Application Administrator that is responsible for their data.
- **Not** allow personnel to enter, change, or delete data from FFIS security tables.
- **Not** be responsible for performing accounting functions within the application.
- Develop detailed written procedures for providing reasonable assurance that all the policies and procedures included in these instructions are adhered to.
- Work with agency staff (i.e., Application Administrator) to create and establish security group definitions.
- Work with agency staff (i.e., Application Administrator) to define individuals to security groups.
- Review logging reports to identify abnormal activities and report these activities to agency management.
- Remove and/or change users' security groups when notified of position change, termination, retirement, death, etc.

Exhibits

[FFIS Application Security Access Request Form](#)

[FFIS Application Security Access Specification Form](#)

1. FFIS Application Security Access Request Form

FFIS INTERNAL SECURITY ACCESS REQUEST FORM																			
User ID: _____					Name: _____														
Phone: _____					Title: _____														
										Organization: _____									
SEC1: _____					SEC2: _____					Application: _____									
New User (Yes/No): _____										CICS Region: _____									
Action Type: _____					Add User _____					Delete User _____					Modify User _____				
Existing Security Group: _____										_____					_____				
_____										_____					_____				
_____										_____					_____				
New Security Group:										_____					_____				
SCAN ACT:										_____					_____				
APPROVAL ACT:										_____					_____				
ENTER ACT:										_____					_____				
CORRECT ACT:										_____					_____				
DELETE ACT:										_____					_____				
SCHED ACT:										_____					_____				
EDIT ONLY ACT:										_____					_____				
HOLD ACT:										_____					_____				
RUN ACT:										_____					_____				
RUN IMMEDIATE ACT:										_____					_____				
FORWHOM TEST TYPE:										_____					_____				
WHERE TEST TYPE:										_____					_____				
WHERE CODE:										_____					_____				
OVERRIDE:										_____					_____				
					1 2 3 4 5					1 2 3 4 5					1 2 3 4 5				
Requesting Official: _____										Date: _____									
Approving Official: _____										Date: _____									
Received by: _____										Date: _____									
Completed by: _____										Date: _____					Log #: _____				

Instructions For Completing The FFIS Application Security Access Request Form

UserID: Enter the ACID assigned to the person who will be set up in the FFIS STAB (security) table. Application Administrators may enter the name of a *model* security profile.

Name: Enter the name of the person who will be set up on the FFIS STAB table.

Phone: Enter your telephone number.

Title: Enter the job title of the person who will be granted the access (e.g., Computer Specialist). This field is optional.

Organization: Enter the name of the organization where the person is employed (e.g., OCFO, NFC, etc.).

SEC1: Enter the (FFIS) division code of the user.

SEC2: Enter the (FFIS) organizational code of the user .

Application: Enter the application name (e.g., FF01 for OCFO implementation, FF02, etc.).

New User: If the user does not have an established NFC userID, enter *Yes*. Otherwise, enter *No*.

CICS Region: Enter the name of the CICS region to be accessed (e.g., CISQ65 for NFC QA environment).

Action Type: Enter whether a person is to be added, deleted, or modified in the STAB (security) table.

Existing Security Group: Enter the name of an existing (previously established) security group or model security profile.

New Security Group: Enter the name of the new security group(s) and the appropriate functions for the group(s).

Approving Official: The owner of the data or a person designated by the owner of the data (e.g., Application Administrator or deputy) must sign here.

2. FFIS Application Security Access Specification Form

**FFIS INTERNAL SECURITY
ACCESS SPECIFICATION FORM
FORM / FORT /FORS TABLE**

Action Type:	<input type="checkbox"/> Add Security Group	<input type="checkbox"/> Delete Security Group
Document Name:	_____	
Table Name:	_____	
Security Groups:	_____	

Requesting Official: (Application Administrator)	_____	Date:	_____
Approving Official: (Owner of Data)	_____	Date:	_____

Received by:	_____	Date:	_____
Completed by:	_____	Date:	_____
		Log #:	_____

Instructions For Completing The FFIS Application Security Access Specification Form For The Form/Fort/Fors Tables

Action Type: Enter a check mark in the appropriate space to add or delete a new security group from the FORM/TABLE.

Document Name: Enter the name of the document for the security group being added or deleted.

Table Name: Enter the name of the table for the security group being added or deleted.

Note: Enter only a document name or a table name, not both.

Security Group(s): Enter the name of the security group(s) being added to or deleted from the table or document.

Requesting Official: The FFIS Application Administrator or another person designated by the data owner must sign here.

Approving Official: The owner of the data or a person designated by the owner of the data must sign here.

Glossary

Access. The authority to use the NFC's computer facilities and the way in which a resource can be used.

ACID. The Accessor ID that identifies a user to CA-Top Secret (TSS). Each user, batch job, or started task has an ACID that identifies both the user and the resources that the user is permitted to access. There are six major types of ACID types; User, Profile, Department, Division, Zone, and Control, together these ACID types create a security hierarchy designed to mirror the typical corporate structure.

Application Image. FFIS database where transaction information is drawn from and stored; each agency will enter and query its data in its own application image.

Applications. The data processing systems operated by NFC. Applications range from the Information Systems, Reporting Systems, Payroll/Personnel Systems, Administrative Payments Systems, Central Accounting Systems, etc., providing the client with input and/or inquiry capabilities.

Batch. A method of processing large amounts of data at one time for jobs too large to perform immediately.

CICS. An acronym for Customer Information Control System, an IBM product. A teleprocessing monitor used for a variety of applications.

CPU. An acronym for Central Processing Unit. The *brain* of the computer, consisting of three basic parts; 1) the control unit, 2) the arithmetic/logic unit, and 3) the storage (main memory) unit. The control unit interprets instructions and issues the appropriate commands to the other two parts, as well as to other computer system devices.

Combination Matrix. A tabular representation of all the possible combinations of the client user access profile identifier and NFC applications (not access level and scope). This is expressed via a horizontal (row) and vertical (column) structure showing the relationship between NFC Applications (i.e., PINQ, SING, etc.) (row) and the variations of the client access profiles (columns) for each job function.

Combination Matrix Identifier. An identification scheme that provides uniqueness and gives some indication as to the access permission included in the profile.

Error Message. A system response that is displayed to inform the user that the entered transaction was not valid, usually providing the reason for the error. All CA-Top Secret messages are prefixed with the character *TSS* and indicate a possible security problem.

Facility. An MVS (Multiple Virtual System) subsystem that processes work on behalf of users and jobs, e.g., TSO, CICS, IDMS, BATCH, etc.

Financial Information Systems Vision and Strategy (FISVIS). A multi-year project initiated by USDA to develop and implement a single, integrated financial information system in USDA, incorporating both financial systems and the financial portions of mixed systems.

Foundation Financial Information System (FFIS). The baseline, or foundation system, for all financial systems in USDA. The FFIS encompasses the financial standards of USDA, the agency and corporate general ledgers, funds control, budget execution and cost accounting/cost accumulation systems of USDA. All financial and the financial portion of mixed systems will be seamlessly integrated with the FFIS when the FISVIS vision is fully realized.

General Prefix. A shorthand way to specify a number of similarly-named resources in the same resource class.

JCL. An acronym for Job Control Language. A method used on IBM mainframe computers to submit jobs to the internal reader (i.e., CPU) for processing.

Masking. A technique that can be used to reduce the number of definitions needed to be defined to CA-Top Secret.

Mode. The security implementation stage that determines the manner in which CA-Top Secret processes resource access requests. The four modes are: FAIL, WARN, IMPLEMENT, and DORMANT.

MVS. An acronym for Multiple Virtual System. The operating system used on the IBM mainframes at NFC.

OFFCTL. A utility that processes documents in batch; allows users to select a given document, a given batch, all documents of a given type, or all documents and batches for processing.

Organizational Structure. The alphanumeric representation for an organization's hierarchical structure, that describes organizational levels such as department, agency, POI/SON, unit, etc.

Ownership. All resources must be *owned* before they can be used and secured in CA-Top Secret data base structure. When a resource is owned by particular ACID, that ACID has unlimited access to the resource. All other ACIDs must be specifically authorized to access the resource.

Password. A unique string of characters associated with a particular user ACID (userID). Signon cannot be successful if an incorrect password is used.

Permission. The process that allows an owned resource to be made available to other users in a controlled manner.

Prefixing. Allows a group of similar resources with the same type to be defined to CA-Top Secret simultaneously.

Profiles. A special ACID type within CA-Top Secret that allows a group of users, performing the same job function, to be permitted the same group of resources.

Resource Items or functions protected by CA-Top Secret such as, a dataset, program, transaction, terminal or facilities.

SEC1. The first-level security group to which a user belongs; used to delimit a user's capabilities within the system; may be configured to correspond to ORG1.

SEC2. The second-level security group to which a user belongs; used to delimit a user's capabilities within the system; may be configured to correspond to ORG2.

Security Access Request. A communication device that is used by the client's ADP Security Officer to notify the NFC's Information Systems Security Officer that some form of access is required for the client's employee(s).

Security Administrator/Information Systems Security Officer. A person designated and authorized to grant users permission to access resources.

TSO. An acronym for Time Sharing Option. Allows two or more users to execute their programs at the same time by dividing system resources among online users.

UserID. An ACID assigned to an individual. The userID is used to signon to the system. See ACID.

Violation. An attempt to access a resource that has not been authorized. A CA-Top Secret error message (i.e., TSSXXE, or TSSXXW) is displayed on the screen and sent to the Audit/Tracking File to record the unauthorized access attempt (violation).

Heading Index

This index provides an alphabetical list of all headings in the procedure. When a heading is referenced, you can use this index to locate the page number.

A

[About This Procedure](#), v
[Access](#), 43
[Access Administration](#), 2
[Access To Facilities](#), 2
[Access To FFIS](#), 56
[Access To Resources](#), 2
[Add Suspend](#), 35
[Amatrix](#), 40
[ASO Panels Or ASO](#), 10
[ASO Primary Option Menu](#), 13

B

[Background](#), 56
[Batch](#), 16

C

[CA-Top Secret](#), 6
[Client Security Officer Activities](#), 3
[Concept Of Security Operation](#), 57

D

[Default](#), 15

E

[Establish User Access](#), 3
[Exhibits](#), 63

F

[FFIS Application Security Access Request Form](#), 65
[FFIS Application Security Access Specification Form](#), 67
[Functions](#), 33

G

[Glossary \(TSS Terms\)](#), 48

H

[Help Screens](#), 9
[HELPAUDT](#), 17
[HELPTSS](#), 18
[HELPUTIL](#), 20
[History](#), 52
[How This Procedure Is Organized](#), v

I

[Instructions For Completing The FFIS Application Security Access Request Form](#), 66
[Instructions For Completing The FFIS Application Security Access Specification Form For The Form/Fort/Fors Tables](#), 68

L

[Lists](#), 42
[Lock](#), 34

M

[Matrix](#), 43
[Messages](#), 50

O

[Officer](#), 44
[Operating Features](#), 9
[Option Selection](#), 9
[Output](#), 31

P

[Password Procedures](#), 5
[Print](#), 45
[Procedure For Establishing And Defining Roles For FFIS Security](#), 57
[Procedures For Acquiring FFIS Access](#), 58
[Procedures For Changes To FFIS Access](#), 59
[Procedures For Requesting Deletion Of FFIS Access](#), 60

R

[REM Suspend](#), 36
[REM Suspend & REP Password](#), 37
[Remote Terminal Usage And Security](#), 7
[REP Password](#), 38
[Responsibilities](#), 1
[Roles And Responsibilities](#), 60

S

[Security Features](#), 6
[Security Policy](#), 1
[Security Procedures](#), 4

[Sign-Off](#), 8
[Sign-On](#), 7
[Standards](#), 53
[System Access](#), 7
[System Overview](#), 1

T

[Telephone Inquiries](#), 4
[TSSALPHA](#), 26
[TSSAUDIT](#), 22
[TSSBATCH](#), 23
[TSSLIST](#), 25, 39, 42
[TSSUTAUD](#), 27
[TSSUTDAY](#), 28
[TSSUTEXT](#), 30
[Tutorial](#), 54
[Tutorial \(Batch\)](#), 32
[Tutorial \(Functions\)](#), 41
[Tutorial](#) (List), 46

U

[Unlock](#), 34

W

[What Conventions Are Used](#), v
[Who To Contact For Help](#), vi
[WHOAMI](#), 34